Gestión del riesgo de SI[1] con base en la norma ISO/IEC 27005:2011 adaptando la metodología MAGERIT V3 para el caso de estudio[23] propuesto

Miguel Ángel Galíndez Muñoz
Jhon Holman Reyes Cerón

Trabajo de pregrado en Ingeniería de Sistemas

Director:
Siler Amador Donado
Especialista en redes y servicios telemáticos

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Grupo de Tecnologías de la Información (GTI)
Línea de Investigación: Seguridad Informática
Popayán, Septiembre de 2016

---

[1] Seguridad de la Información
[2] Caso de estudio: procedimiento de *Formulación y ejecución de proyectos con financiación externa* adscrito a la *Vicerrectoría de Investigaciones (VRI)* de la Universidad del Cauca.
[3] Cabe resaltar que el presente trabajo se caracteriza por ser un estudio observacional y que, por ende, el término "*caso de estudio*" hará referencia al procedimiento que será observado. Para mayor información, ver la sección 1.1.

Gestión del riesgo de SI con base en la norma ISO/IEC 27005:2011 adaptando la metodología MAGERIT V3 para el caso de estudio propuesto

Trabajo de pregrado presentado a la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca para la obtención del título de Ingeniero de Sistemas

Miguel Ángel Galíndez Muñoz
Jhon Holman Reyes Cerón

Director:
Siler Amador Donado
Especialista en redes y servicios telemáticos

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Popayán, Cauca, Septiembre de 2016

Agradecimientos

Como siempre debe ser, agradecemos primero a Dios y a la Santísima Virgen María por todas las bendiciones y ayuda que hemos recibido a lo largo de nuestras vidas y, en especial, por todos los favores que se nos han concedido durante nuestros estudios universitarios.

Cómo no agradecer a nuestros padres, esas personas que siempre han estado a nuestro lado, tanto en los momentos felices como en las angustias y adversidades. en sadasd

Resumen estructurado

Para hacer frente a las diversas amenazas de SI a las que se expone la Universidad del Cauca, la administración ha decidido implantar un SGSI, siguiendo la norma ISO/IEC 27001, con el fin de proteger los activos de información pertenecientes a la institución, dando prioridad a los procedimientos que, como el caso de estudio, son denominados ‘críticos’.

Para atender las necesidades del caso de estudio en materia de la SI, el presente proyecto pretende adaptar la metodología MAGERIT V3 como un mecanismo que permita gestionar, adecuadamente, los riesgos de la SI en el caso de estudio, de acuerdo con los requerimientos de la norma ISO/IEC 27001. Para obtener su validación, dicha adaptación será evaluada y sometida a los ajustes necesarios para corregir las fallas identificadas. Además, por recomendación del estándar ISO/IEC 27003, este proyecto deberá desarrollar la planeación de un SGSI para el caso de estudio con el fin de garantizar la idoneidad de la gestión de los riesgos de la SI.

Para lograr los objetivos propuestos, el presente proyecto se estructura en cuatro etapas de desarrollo: en la primera de ellas se analizará el dominio del problema mediante la ejecución la primera fase de la planeación de un SGSI, en la segunda se identificaran los aspectos esenciales relacionados con la construcción de la adaptación de MAGERIT V3 mediante la ejecución de las fases 2 y 3 de la planeación de un SGSI, en la tercera se construye la adaptación y, finalmente, en la cuarta etapa se ejercita la adaptación propuesta y se corrigen las fallas identificadas mediante la ejecución de la cuarta fase de la planeación de un SGSI.

Como resultado, se logró desarrollar la planeación de un SGSI para el caso de estudio y se obtuvo la adaptación satisfactoria de MAGERIT V3, la cual permitió identificar que el caso de estudio se encuentra expuesto a un alto nivel de riesgo. Frente a ello, se desarrolló un Plan de Tratamiento de Riesgos y una Declaración de Aplicabilidad.

Para concluir, se resalta que los riesgos fueron valorados y tratados satisfactoriamente y que, para poder adaptar MAGERIT V3 al caso de estudio, fue necesario agregarle 8 nuevas actividades al enfoque ofrecido por dicha metodología y ajustar el orden de ejecución de sus tareas.

Palabras claves: SGSI, SI, gestión de riesgos, salvaguardas, amenazas, activos, riesgos.

Contenido

Pág.

Lista de figuras

Lista de tablas

Glosario

Activo: recurso o funcionalidad necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Algunos ejemplos son: información, datos, servicios, aplicaciones (software), equipos (hardware), redes de comunicaciones, recursos humanos e instalaciones físicas.

Amenaza: causa potencial de un incidente que puede resultar en daños y perjuicios para la organización.

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza. Generalmente se traduce en el valor que pierde el activo.

Integridad: Propiedad o característica consistente en que la información y los activos asociados no sean alterados de manera no autorizada

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Salvaguarda: procedimiento, control o medida cuyo propósito es reducir el nivel de riesgo al que se encuentran sometidos los activos de información de la organización. Es equivalente al término *"**control**",* usado por los estándares de la serie ISO 27000.

Trazabilidad: característica de seguimiento que permite asociar, inequívocamente, a un individuo o entidad, todas sus acciones realizadas.

Vulnerabilidad: Defectos o ausencia de los controles necesarios para gestionar la SI, lo cual propicia la materialización de las amenazas.

Abreviaturas

Caso de estudio: procedimiento de *Formulación y ejecución de proyectos con financiación externa* adscrito a la Vicerrectoría de Investigaciones de la Universidad del Cauca.

CDP: Certificado de Disponibilidad Presupuestal.

CISO: Chief Information Security Officer – Oficial de Seguridad de la Información

FPL: Finanzas Plus; un sistema de información moderno, modular e integrado construido para apoyar la gestión, control y administración de los recursos financieros de organizaciones pertenecientes al sector estatal.

GESPROY: Sistema de Gestión y Monitoreo a la Ejecución de Proyectos

MAR: Método de Análisis de Riesgos.

MARA: Método de Análisis de Riesgos Adaptado.

OPS: Orden de Prestación de Servicios

OTAN: Organización del Tratado del Atlántico Norte.

PDCA: siglas en inglés que hacen referencia la ciclo Deming: Plan – Do – Check - Act

PTR: Plan de Tratamiento de Riesgos

SGSI: Sistema de Gestión de la Seguridad de la Información

SI: seguridad de la información

SIVRI: sistema de información de la Vicerrectoría de Investigaciones de la Universidad del Cauca

SOA: Statement Of Applicability (Declaración de Aplicabilidad)

SRF: Sistema de Recursos Físicos; una aplicación modular e integrada construida para apoyar la administración de recursos físicos de empresas estatales.

TIC: Tecnologías de la Información y las comunicaciones

UPS: Sistema de alimentación ininterrumpida

VRI: Vicerrectoría de Investigaciones de la Universidad del Cauca

Capitulo 1

Introducción

1.1. Definición de caso de estudio

Para entender el significado que el término *"caso de estudio"* tiene para el presente proyecto, resulta conveniente que, en primer lugar, se hable de los estudios empíricos como método de investigación. En [59] son definidos como un acto u operación encaminada a descubrir algo desconocido mediante la obtención y análisis de datos. Según los autores de [69], los métodos de investigación empíricos son cruciales, pues permiten incorporar el comportamiento humano al interior del enfoque de investigación, suministrando, de esa manera, una importante base científica para diferentes disciplinas como la Ingeniería del Software.

En [64] se declara que los estudios empíricos son necesarios para desarrollar o mejorar procesos, métodos y herramientas, e incluso, en [69], son calificados como una herramienta esencial para los investigadores[4]. En relación con lo anterior, los autores de [65] manifiestan que es evidente que la aceptación de los métodos empíricos y sus contribuciones está en continuo crecimiento, lo cual es demostrado por los autores de [62], quienes exponen unas cifras que evidencian la creciente aceptación de los estudios empíricos en comparación con la década de los 90s.

En [59], se expone una amplia recopilación de la información disponible sobre los diferentes tipos de documentos publicados en revistas y conferencias relacionadas con la Ingeniería del Software. Gracias a ello, y a lo expuesto por [63, 64], se logró identificar la clasificación de los estudios empíricos que proponen los autores de [60], quienes, examinando múltiples ejemplos de validación de tecnologías, desarrollaron una taxonomía que describe 12 enfoques para la experimentación. Los autores de [60] clasifican estos 12 tipos de estudios empíricos en 3 categorías, como se describe a continuación:

[4] Según los autores de [69], los estudios empíricos proveen efectos positivos como la divulgación del conocimiento

- Históricos: consiste en recolectar datos de proyectos que ya han sido completados y, a su vez, se clasifican en: búsqueda de la literatura, datos heredados, lecciones aprendidas y análisis estático. Según [61], los métodos históricos son preferidos cuando no hay prácticamente ningún acceso o control sobre el entorno y los comportamientos relevantes como el proceso de desarrollo. La contribución distintiva de este método es la investigación sobre hechos pasados; cuando no hay personas vivas a quien entrevistar, confiando únicamente en documentos y artefactos culturales como principales fuentes de evidencia.

- Controlados: proveen múltiples instancias de una observación con el fin de obtener la validación estadística de los resultados. Según [61], los métodos controlados se caracterizan por ejercer un control directo, preciso y sistemático del entorno y de los comportamientos relevantes como el proceso de desarrollo. Un claro ejemplo de estos estudios son los experimentos de laboratorio, en los cuales el investigador puede enfocarse en una variable, controlando el comportamiento de los demás factores que están por fuera del alcance de interés.

- Observacionales: recolectan datos relevantes a medida que el proyecto se va desarrollando. Según [61], los métodos observacionales son preferidos cuando se examinan eventos contemporáneos sobre los cuales no se puede ejercer mayor control del entorno y de los comportamientos relevantes como el proceso de desarrollo. De la misma manera, los autores de [61], manifiestan que estos métodos confían en las mismas técnicas que los métodos históricos pero agregando dos contundentes fuentes de evidencia: la observación directa de los eventos estudiados y las entrevistas a las personas involucradas.

Partiendo de las definiciones identificadas anteriormente y de acuerdo con [61, 63], resulta válido considerar el presente proyecto como un estudio observacional, aclarando que el término *observacional* hará referencia a recolectar información acerca del sujeto de nuestro estudio en una situación donde no tenemos un estricto control sobre el entorno y los comportamientos relevantes como el proceso de desarrollo.

Según [60], un estudio observacional puede ser un estudio de caso, un estudio de campo, un monitoreo de proyectos o una afirmación. Esta tipificación es descrita por los autores de [60] como se muestra a continuación:

- Monitoreo de proyecto: representa el más bajo nivel de experimentación y medición. Consiste en recolectar y almacenar los datos obtenidos durante el desarrollo del proyecto. Este método carece de cualquier objetivo experimental y consistencia en los datos recolectados.

- Estudio de caso. Los investigadores monitorean un proyecto y recolectan datos. A diferencia del anterior, éste se deriva de los objetivos específicos del proyecto.

- Estudios de campo: puede examinar simultáneamente datos recolectados que provengan de varios proyectos.

- Afirmaciones: según [59] consiste en un proyecto en el cual los desarrolladores son, a la vez, los experimentadores y los objetos estudiados, lo cual genera una alta probabilidad de que se presente parcialidad en los resultados del estudio. Por lo anterior, muchos autores, como los de los documentos [60, 65, 66], coinciden en que éste no es un método de investigación apropiado.

Contrario a esta tipificación de los estudios observacionales, propuesta en [60]:

- Los autores de [59] consideran que los estudios observacionales son diferentes de los estudios de caso y de los estudios de campo.

- Los autores de [65] prefieren ver el monitoreo de proyectos como una parte de un estudio de caso y los estudios de campo como múltiples estudios de caso.

- Los autores de [59] afirman que es muy difícil distinguir entre los estudios de caso y los reportes de experiencia[5].

Lo anterior evidencia una clara discrepancia entre distintos autores de la literatura en cuanto a la tipificación de los estudios observacionales. Ante esta situación de incertidumbre, resulta conveniente considerar el presente proyecto como un estudio observacional en su definición conceptual más general, sin estructurarlo como uno de los tipos específicos mencionados anteriormente.

En virtud de lo señalado y con base en la definición propuesta en [61][6], el término *"caso de estudio",* en el presente proyecto, hará referencia a la entidad que será objeto de la investigación de éste estudio observacional que, para esta ocasión, corresponde al procedimiento: *Formulación y ejecución de proyectos con financiación externa,* adscrito a la VRI.

Las anteriores aseveraciones se fundamentan en el hecho de que:

- Según [65], un estudio de caso es, en esencia, puramente observacional.
- Según [69], un estudio de caso es un estudio observacional.
- Según los autores de [65], el término caso de estudio es usado en paralelo con términos como estudio de campo y estudio observacional.

[5] Los reportes de experiencias son un ejemplar de los métodos de investigación empíricos de tipo históricos

[6] El autor de [61] define el "*caso"* como un sujeto, entidad concreta, evento, ocurrencia o acción

1.2. Presentación del trabajo

La información es uno de los activos más importantes en una organización, por ende ésta debe ser protegida para garantizar la competitividad y la continuidad del negocio. En respuesta a esa necesidad surge la Seguridad de la Información, en adelante "*SI*". No obstante, el avance de las tecnologías y su generalizado uso han dado lugar a nuevas y variadas amenazas, las cuales por lo general explotan las vulnerabilidades expuestas, causando daños y perjuicios a la organización. El riesgo asociado a la SI, en adelante "riesgo", siempre estará presente, razón por la cual se debe, constantemente, velar por la *Confidencialidad, Integridad* y *Disponibilidad* de la información y los activos que la soportan.

La Universidad del Cauca, por su parte, se encuentra conformada por 535 funcionarios administrativos, 561 docentes[7], 10436 estudiantes de pregrado y 598 estudiantes de posgrado[8], de los cuales retiene información sensible como datos personales, bancarios, entre otros. Adicionalmente, esta institución manipula grandes volúmenes de documentación inherente a los procesos de negocio, como por ejemplo, informes presupuestales, contratos y cuentas bancarias. En un mundo interconectado, esta información y los activos asociados, se ven enfrentados a un amplio espectro de amenazas que van desde el espionaje y fraude electrónico hasta ataques de denegación de servicio, entre otros. Bajo estas circunstancias, es muy probable que la información se vea comprometida en situaciones en las que puede ser borrada, divulgada, manipulada, o suplantada, afectando gravemente la legitimidad, prestigio y el buen nombre de la Universidad del Cauca, la cual, muy posiblemente, se verá enfrentada a serios inconvenientes legales.

Reconociendo la evidente necesidad de adquirir y preservar la SI, la Universidad del Cauca emprende el proyecto "Implantación y certificación del Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad del Cauca", el cual fue aprobado mediante la resolución número R-005 de 2015, emitida por la Rectoría de la institución, resolviendo que se debe dar inicio a la implantación del SGSI. En relación con lo anterior, algunas dependencias de la Universidad del Cauca han manifestado su interés por la iniciativa, una de ellas ha sido la Vicerrectoría de Investigaciones (VRI), la cual postula la *Formulación y ejecución de proyectos con Financiación Externa,* en adelante *caso de estudio*, como un procedimiento crítico a tener en cuenta.

En el marco del proyecto del SGSI de la Universidad del Cauca y en respuesta a la necesidad de adquirir y preservar la SI en el caso de estudio, la norma ISO/IEC 27001

[7] Datos suministrados por Fredy Pacheco Vidal, División de Gestión del Talento Humano, Universidad del Cauca

[8] Datos correspondientes al Segundo semestre del año 2013. Suministrados por la Oficina de Planeación y Desarrollo Institucional en su Boletín Estadístico de 2013

[2] establece que se debe llevar a cabo una gestión de riesgos de la SI siguiendo el estándar ISO/IEC 27005 [5]. Sin embargo, [5] no brinda ninguna metodología específica para tal fin, siendo responsabilidad de cada organización especificar el enfoque que mejor se ajuste a su contexto, necesidades y objetivos.

En virtud de lo señalado, se decide utilizar una de las tantas metodologías disponibles: MAGERIT V3[9]. Esta fue elaborada por el Consejo Superior de Administración Electrónica de España y se encuentra alineada con el estándar ISO/IEC 27005 [5], tiene un amplio ámbito de aplicación a nivel internacional y además cuenta con la herramienta de apoyo PILAR [11], cuyo desarrollo es patrocinado por el Centro Criptológico Nacional de España.

No obstante, de lo anterior, surge el interrogante: ¿cómo adaptar la metodología MAGERIT V3 al caso de estudio propuesto?

1.3. Justificación

¿Por qué, en la VRI, se considera el caso de estudio como un aspecto crítico? Una de las responsabilidades de este procedimiento es velar por la correcta inversión de los recursos externos recibidos que, en el presente, pueden llegar a superan los 100.000 millones de pesos[10]. Una vez realizado el registro, la Universidad del Cauca adquiere la obligación contractual de culminar el proyecto bajo una fecha de entrega establecida. De ese modo, si no se ejecutan adecuadamente los recursos, la Universidad se verá obligada a responder por la entrega del proyecto terminado y asumir las consecuencias legales y financieras que de ello se deriven. Adicionalmente, los diferentes órganos de control y vigilancia del estado, como por ejemplo, la Contraloría General de la Republica[11], están en la facultad de intervenir en cualquier momento a la Universidad del Cauca. El hallazgo de cualquier irregularidad en las actividades y el manejo de los recursos implicarían serios inconvenientes legales.

Toda la responsabilidad que recae sobre este procedimiento, y el eventual impacto a la Universidad ocasionado por cualquier anomalía en sus operaciones, refleja la necesidad de gestionar los riesgos de la SI. A pesar de ello, en la VRI se desconoce la gestión de los riesgos asociados a la SI, hasta tal punto que ni siquiera hay un concepto claro del verdadero valor de sus activos, ni mucho menos, un conocimiento de las amenazas a las que se enfrentan. Bajo estas condiciones, la VRI no cuenta con

[9] Para mayor información, visitar http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vvw-jPl97IU

[10] Cifra suministrada por Helder Mauricio Chacón Villota, Jefe de la División de Gestión de la Investigación, VRI.

[11] Dado el caso de que se disponga de recursos y bienes públicos.

la capacidad para proteger sus propios activos de información, para los cuales no podrá garantizar la confidencialidad, integridad, ni la disponibilidad.

1.4. Estado del arte

En respuesta a la situación del caso de estudio, el estándar ISO/IEC 27005 [5] ofrece, con base en los requerimientos de la norma ISO/IEC 27001 [2], los lineamientos y directrices para conducir una adecuada gestión de los riesgos de la SI, permitiendo mitigarlos para, finalmente, lograr un nivel adecuado de SI.

Generalmente, la serie de normas ISO 27000 propone la implantación de un SGSI como solución a las necesidades asociadas a la SI. Dicha implantación debe cumplir con los requerimientos establecidos por la norma ISO/IEC 27001 [2] y puede ser lograda siguiendo el modelo PDCA (Plan, Do, Check, Act) para la mejora continua, también conocido como ciclo Deming [6, 7, 8].

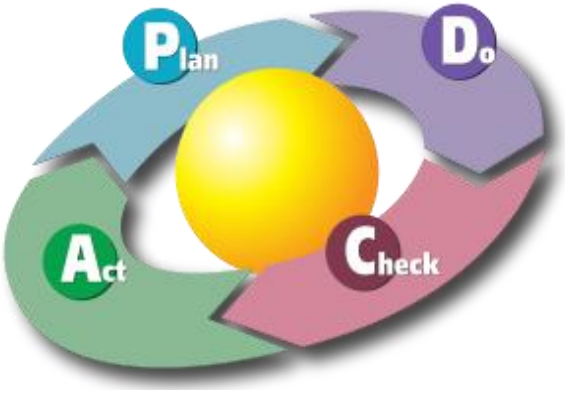

Figura 1.1. Ciclo Deming.
Tomada de [9]

- **PLANEAR (PLAN)**. Corresponde a la planeación del SGSI[12]. El estándar ISO/IEC 27003 [4], sugiere abordar lo siguiente:

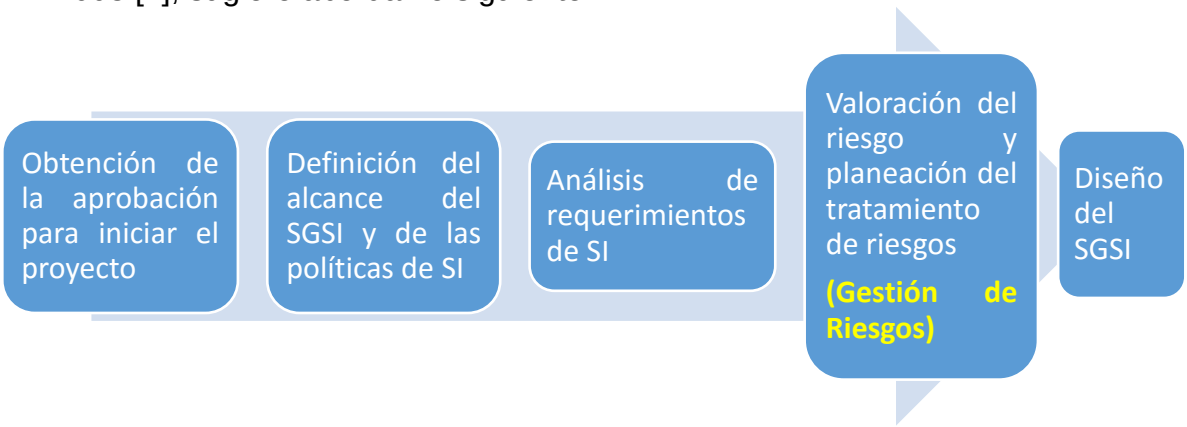

Figura 1.2. Fases de la planeación de un SGSI. Tomada de [4]

El *Diseño del SGSI,* definido por el estándar ISO/IEC 27003, tiene por objetivo complementar el plan de implementación del SGSI con la definición de los

[12] También conocida como fase *PLAN* de la implantación de un SGSI

requerimientos para el control de documentación y la implementación de controles asociados a las TIC, procesos del negocio y requerimientos del SGSI. Como resultado, se logra desarrollar:

- ✓ Planes de auditorías.
- ✓ Procedimiento de control de registros.
- ✓ Plan de implementación de controles (procedimientos de acciones correctivas o preventivas)
- ✓ Demás planes y procedimientos operativos de la implementación del SGSI como el programa de educación y entrenamiento, etc.

En relación con lo anterior, el Foro de Implementación ISO27k, una comunidad global conformada por más de 3.000 profesionales de la SI; miembros de la norma ISO/IEC, gestores de la SI, analistas, CISOs, auditores, consultores y estudiantes de maestría y doctorado[13], sugiere que el *Diseño del SGSI* sea abordado durante la implementación del SGSI[14] y no durante la planeación del mismo. Como evidencia de lo anterior, en [10], esta comunidad de expertos propone un proceso para la implementación y certificación de un SGSI cuya actividad número 6 se caracteriza por perseguir los mismos fines del *Diseño del SGSI* y que, según la leyenda suministrada por [10], corresponde a una tarea que se deberá abordar durante la implementación del SGSI.

Teniendo en cuenta la idoneidad, experiencia y conocimiento de los miembros del Foro de Implementación ISO27k, se decide aceptar la anterior sugerencia, por lo cual, en adelante, la planeación del SGSI no incluirá el Diseño del SGSI. Esto es posible ya que el estándar ISO/IEC 27003 no define ningún requisito, limitándose solamente a dar recomendaciones y por ende, la anterior propuesta no representará ningún incumplimiento.

- **HACER (DO)**. Ejecutar e implementar lo establecido por la planeación del SGSI.

- **VERIFICAR (CHECK)**. Comparar los resultados planeados con los resultados obtenidos.

- **ACTUAR (ACT)**. Tomar acciones correctivas sobre el SGSI.

Lo anterior evidencia que la gestión de los riesgos de la SI hace parte de la planeación de un SGSI, y que sólo puede iniciarse una vez se hayan definido el alcance, la política y los requerimientos de SI. Cabe recalcar que, si bien el estándar ISO/IEC 27005 [5]

[13] Los miembros de esta comunidad se caracterizan por ser usuarios activos de la serie de normas ISO/IEC 27000 dispuestos a compartir su conocimiento y experiencia con la comunidad, y aquellos que están dando sus primeros pasos hacia la adopción de las normas.
[14] Corresponde al paso HACER del modelo PDCA.

provee las directrices para una correcta gestión de riesgos, este no define ninguna metodología específica para tal fin, siendo responsabilidad de cada organización especificar el enfoque que mejor se ajuste a su contexto, necesidades y objetivos.

En virtud de lo señalado, se procede a ejecutar una revisión sistemática de la literatura, con base en los métodos propuestos en [76-80], con el propósito de buscar documentos relacionados con las fases de la planeación de un SGSI, en especial, con la gestión de riesgos y las respectivas metodologías que actualmente se encuentren disponibles. A continuación, se presentan los resultados de la revisión de la literatura, agrupados de acuerdo a la procedencia de los documentos: ámbito internacional, nacional o regional, según corresponda.

1.4.1. Ámbito Internacional.

En [81, 82] se provee información general sobre cada uno de los estándares que componen la serie de normas ISO 27000. En [83] se presenta una introducción detallada a la planeación del SGSI, la cual establece como obligatoria la definición de la política para dicho sistema de gestión.

La planeación de un SGSI también incluye la gestión de riesgos. Tal gestión es considerada como un componente crucial para la práctica de la SI, debido a que sus resultados son la base sobre la cual la gerencia toma decisiones frente a cada riesgo identificado [84]. En los trabajos de investigación [85, 86] se confirma su importancia en la protección de los activos de la información, resaltando que las amenazas aumentan cada día. Actualmente, [5] es el estándar dedicado a la gestión de riesgos de la SI, y en torno a este se encuentran disponibles variadas metodologías, como es el caso de MAGERIT.

Frente a la diversidad de metodologías disponibles, es natural que surja la necesidad de conocer y comparar estos distintos enfoques a fin de encontrar el que represente la mejor opción. Así por ejemplo, la OTAN[15] publicó el reporte técnico [14] en el cual menciona las metodologías que recomienda para sus países aliados, entre las cuales se destaca a MAGERIT y su herramienta de apoyo PILAR. Además, en la publicación científica [15] se evidencia la superioridad de MAGERIT frente a otras ocho metodologías que fueron evaluadas midiendo el nivel de correspondencia y satisfacción de los elementos de las TIC.

Adicionalmente, en [14] se da a conocer que MAGERIT permite un análisis de riesgos, ya sea cualitativo o cuantitativo. Frente a ello, en [46] los autores exponen un cuadro comparativo entre los dos tipos de análisis. Según ellos, se debe contemplar ambos enfoques en lugar de centrarse solo en uno, proponiendo que se debe realizar una primera valoración con el enfoque cualitativo buscando identificar sectores críticos y luego realizar una segunda iteración con el enfoque cuantitativo para lograr una mayor

[15] Organización del Tratado del Atlántico Norte

precisión. Otro motivo para no dejar de lado el análisis cualitativo es que, cuando los recursos destinados para el proyecto son limitados, este enfoque representa la única opción viable [46]. Los autores de [43, 44, 45] manifiestan su interés por un análisis de riesgos cuantitativo. Expresan que solo así se logra mayor precisión en los resultados del valor del riesgo, además el impacto a la organización quedará expresado en términos financieros, permitiendo un mejor análisis.

En [87] los autores plantean la necesidad de que las empresas puedan compartir las lecciones aprendidas una vez ocurren los incidentes de seguridad, manifestando que un conocimiento compartido sería de gran utilidad para la gestión de riesgos. Como solución, los autores proponen implementar una plantilla genérica de seguridad, también denominada como GST, por su acrónimo en inglés (Generic Security Template).

1.4.2. Ámbito Nacional

A nivel nacional se han desarrollado trabajos como [88], [89], [21] y [90] donde los autores comparan distintas metodologías para la gestión de riesgos, resaltando las características más relevantes, de cada una, con el fin de identificar las mejores prácticas. En [21], con la intención de encontrar la opción más adecuada, los autores aplican, a la empresa ECO-VOLTIO, distintas técnicas para la gestión de riesgos, logrando determinar que MAGERIT resulta ser la opción más efectiva y completa ya que protege la información en cuanto a integridad, confidencialidad, disponibilidad y otras características importantes para garantizar la SI.

1.4.3. Ámbito Regional

En [12] se evidencia la conducción del análisis y gestión de riesgos en una dependencia de la Universidad del Cauca. Los autores usaron la Metodología de las Elipses [13] para definir el alcance del proyecto y adaptaron la metodología OCTAVE-S para la gestión del riesgo. Por otra parte, en [20] los autores realizaron un trabajo similar al anterior, pero éste aplicado al Colegio Mayor del Cauca y tomando como marco de referencia a la metodología MAGERIT V3.

1.4.4. Conclusiones del estado del arte

La revisión de la literatura permitió identificar que la gestión de riesgos es vital para la SI, pues en base a sus resultados se seleccionan las contramedidas que harán frente a las amenazas, para que de ese modo, se logre mitigar los riesgos [84]. Siguiendo los lineamientos de la familia de normas ISO 27000 y adoptando el modelo PDCA [6, 7, 8], dicha gestión termina siendo parte de la planeación del SGSI, la cual, en conformidad con la guía suministrada por el estándar ISO/IEC 27003 [4], deberá incluir las siguientes fases:

- Obtención de la aprobación para iniciar el proyecto.
- Definición del alcance del SGSI y de las políticas de SI.
- Análisis de requerimientos de SI.
- Valoración del riesgo y planeación del tratamiento de riesgos (Gestión de Riesgos)

Lo anterior evidencia que, para poder gestionar los riesgos de la SI en el caso de estudio, se deberá abordar la fases comprendidas por el proceso de planeación de un SGSI, de acuerdo con las recomendaciones suministradas por el estándar ISO/IEC 27003 [4]. Se debe recordar que, por recomendación del Foro de Implementación ISO27k, el *Diseño del SGSI* no será parte de la planeación del SGSI[16].

De igual manera, se identifica que la guía proporcionada por el estándar ISO/IEC 27003 [4] no define metodologías específicas para el desarrollo de cada una de las fases comprendidas por la planeación de un SGSI. Frente a ello, la revisión del estado del arte permitió, oportunamente, identificar que:

- Para la definición del alcance del SGSI, los autores de [12] sugieren usar la Metodología de las Elipses, la cual es originalmente propuesta en [13]. Debido a la similitud del presente proyecto con el trabajo hecho en [12], se decide emplear esta metodología para dicha finalidad.

- Para la definición de las políticas de SI, puede resultar útil considerar el trabajo realizado en [20], en el cual se evidencia un completo y amplio ejemplar de una política de SI.

- Para la gestión de riesgos, los autores de [21] llegan a la conclusión de que MAGERIT V3 es la metodología más adecuada, argumentando que esta le otorga a las organizaciones una mayor asertividad en la toma de decisiones, debido a que su análisis de riesgos es el más completo, pues considera elementos empresariales que otras metodologías no contemplan. Asimismo, en los trabajos de pregrado [16-19] y en los trabajos de posgrado [20, 21], se evidencia la aplicación satisfactoria de la metodología en distintos tipos de entidades, destacando un factor común, el uso de PILAR. En virtud de lo señalado, se eligió a MAGERIT V3 como marco de referencia para el presente proyecto y a PILAR como herramienta de apoyo a la gestión de riesgos.

Por último, en [87] los autores proponen adoptar las Plantillas Genéricas de Seguridad, recalcando la importancia de compartir lo aprendido sobre los incidentes de seguridad, una vez éstos ocurren.

[16] Para mayor información, retomar el inicio de la sección 1.4

1.5. Contribución del trabajo

- Guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3 para la gestión de riesgos de la SI en procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca.

- Desarrollo de la planeación de un SGSI, para el caso de estudio, con base en la norma ISO/IEC 27001:2013 [2] y al cumplimiento de los requerimientos que en ella se estipulan.

- Guía para la implementación del mecanismo de comunicación de problemas en la SI: Plantillas Genéricas de Seguridad, como una propuesta para que las dependencias de la Universidad del Cauca logren un aprendizaje colaborativo sobre los incidentes de SI.

1.6. Objetivos

1.6.1. Objetivo general

Adaptar la metodología MAGERIT V3 como mecanismo para la gestión de riesgos de la SI, según los requerimientos de la norma ISO/IEC 27001 [2], en el caso de estudio propuesto.

1.6.2. Objetivos específicos

1. Desarrollar la planeación de un SGSI, con base en el cumplimiento de los requisitos del estándar ISO/IEC 27001 [2] y siguiendo las fases establecidas por el estándar ISO/IEC 27003 [4], para el caso de estudio propuesto.

2. Evaluar la adaptación de la metodología MAGERIT V3, propuesta durante la planeación del SGSI, como mecanismo para la gestión de riesgos de SI en el caso de estudio.

3. Ajustar la adaptación de la metodología MAGERIT V3, propuesta durante la planeación del SGSI, como mecanismo para la gestión de riesgos de SI en el caso de estudio.

1.7. Metodología

Como se discutió en la sección 1.1, el presente proyecto corresponde a un estudio observacional que, de acuerdo con las definiciones suministradas por [61, 63], deberá recolectar información acerca de nuestro caso de estudio[17] en una situación donde, según [60], aparte de los cambios a la nueva tecnología que será estudiada[18], habrá poco control sobre el entorno y los comportamientos relevantes como el proceso de desarrollo.

En razón de lo expuesto, para el desarrollo del proyecto se toma como marco de referencia el modelo propuesto en [25] que, según su autor, se ajusta a proyectos de cualquier índole cuyo objetivo sea construir una solución oportuna y de calidad. Este modelo divide el desarrollo en cuatro etapas: estudio de pre-factibilidad, formulación, ejecución y validación de la solución.

Con base en el modelo citado y teniendo en cuenta que, para poder gestionar los riesgos de la SI en el caso de estudio, se debe abordar las fases comprendidas por el proceso de planeación de un SGSI[19], el desarrollo del presente proyecto se estructura de la siguiente manera:

ETAPA	DESCRIPCIÓN	CUMPLIMIENTO DE LOS OBJETIVOS DEL PROYECTO
Estudio de pre-factibilidad	Etapa desarrollada en el capítulo 3. Su propósito es analizar el dominio del problema y determinar si se puede continuar con el proyecto. Cabe recordar que el problema estudiado por el presente trabajo es: *"¿Cómo adaptar la metodología MAGERIT V3 para lograr gestionar los riesgos de la SI en el caso de estudio?"* El análisis del dominio del problema es llevado a cabo mediante la ejecución de las actividades de la primera fase del proceso de planeación de un SGSI expuesto por la Figura 2.2, de las cuales se obtiene el *Caso de Negocio*: un entregable que permite esclarecer las características, prioridades y	Aporta al cumplimiento del primer objetivo específico, pues logra abordar la primera fase del proceso de planeación de un SGSI, expuesto por la Figura 2.2.

[17] El término "caso de estudio", en el presente proyecto, hará referencia a la entidad que será objeto de la investigación de éste estudio observacional que, para esta ocasión, corresponde al procedimiento: Formulación y ejecución de proyectos con financiación externa, adscrito a la VRI. Para mayor información, retomar la sección 1.1.

[18] Para efectos del presente proyecto, corresponde a la metodología para la gestión de riesgos: MAGERIT V3

[19] Dicha afirmación fue una de las conclusiones del estado del arte.

	requerimientos del caso de estudio en materia de la SI. El caso de negocio se entrega al usuario de la adaptación, el jefe de la División de Gestión de Investigación, quien concede el concepto viable y el visto bueno del mismo. De esta manera, el análisis del dominio del problema es abordado por el entregable *Caso de Negocio,* expuesto por la sección 3.1. Luego, en el contexto académico del presente proyecto, el Consejo de Facultad de la FIET, después de aprobar el anteproyecto del presente trabajo de pregrado, es quien determina la viabilidad del proyecto. Añadiendo que este proyecto está enmarcado dentro del Proyecto de Implantación del SGSI para la Universidad del Cauca. Como evidencia de lo anterior, la propuesta y la respectiva aprobación del proyecto, son discutidas por las secciones 3.2 y 3.3. De esta manera, la presente etapa logra abordar la primera fase del proceso de planeación de un SGSI.	
Formulación del proyecto	Etapa desarrollada en el capítulo 4. Su propósito es analizar los aspectos esenciales relacionados con la construcción de la solución y el aseguramiento de su viabilidad. Según el estándar ISO/IEC 27003 [4], los factores claves para el desarrollo exitoso del proyecto son: • La definición del alcance del SGSI y de las políticas de SI. Estos aspectos son abordados, respectivamente, por las secciones 4.1 y 4.2. • • El análisis de requerimientos de la SI. Útil para identificar los activos cubiertos por el alcance y obtener una idea general del estado actual de la SI en el caso de estudio. Para ver los resultados del análisis de requerimientos de SI, diríjase a la sección 4.3. Para identificar el alcance de manera adecuada se acude al usuario de la adaptación quien, en su calidad de encargado de la adaptación, aprueba las políticas de SI formuladas y concede información útil para la definición de los requerimientos de SI del caso de estudio. De esta manera, la presente etapa	Aporta al cumplimiento del primer objetivo específico, pues logra abordar las fases 2 y 3 del proceso de planeación de un SGSI, expuesto por la Figura 2.2.

	logra abordar las fases 2 y 3 del proceso de planeación de un SGSI expuesto por la Figura 2.2, satisfaciendo, de igual manera, los respectivos entregables.	
Ejecución del proyecto	Etapa desarrollada en el capítulo 5. Su propósito es construir la solución del proyecto. Cabe recordar que la solución al problema estudiado por el presente trabajo es: *"la adaptación de la metodología MAGERIT V3 como mecanismo para la gestión de los riesgos de la SI en procedimientos, que como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca"*. Primero que todo se consulta al usuario de la adaptación en los temas relacionados con la legislación aplicable al caso de estudio y demás características del contexto. Luego, para poder adaptar MAGERIT V3 se agregan 8 nuevas actividades al *Método de Análisis de Riesgos* (MAR) propuesto por esta metodología. Dichas actividades son descritas por las secciones 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.3.1, 5.4.1, 5.4.2 y 5.4.5. Además, se ajusta el orden de ejecución de las actividades originalmente propuestas por MAGERIT V3, pues, como lo identificó la sección 2.3.2, ésta metodología incumplía los requerimientos de la norma ISO/IEC 27001 [2] cuando establecía que se debían seleccionar las salvaguardas (controles) antes de estimar y priorizar los riesgos. Como producto de estas adaptaciones propuestas, se obtiene el *Método de Análisis de Riesgos Adaptado* (MARA), el cual es ilustrado por la Figura 5.2 y descrito por las secciones 5.1, 5.2, 5.3 y 5.4. Para esclarecer los cambios propuestos por el MARA, la Figura 5.1 ilustra la metodología MAGERIT en su versión original y la Tabla 5.1 ilustra una confrontación entre estas dos versiones. Adicionalmente, se desarrolla la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, con el propósito de brindar orientación y soporte a la aplicación del MARA.	Aporta al cumplimiento del primer objetivo específico, pues desarrolla la adaptación de la metodología MAGERIT V3, lo cual será el insumo principal para que, en la siguiente etapa de desarrollo del proyecto, se ejecute la cuarta y última fase del proceso de planeación de un SGSI, expuesto por la Figura 2.2.

Validación de la solución	Etapa desarrollada en el capítulo 6. Su propósito es ejercitar la solución y corregir los errores que se detecten. De acuerdo con lo anterior, se debe usar el MARA, producto de las adaptaciones hechas a la metodología MAGERIT V3, para ejecutar la fase 4 del proceso de planeación de un SGSI, expuesto por la Figura 2.2. Como evidencia de ello, la sección 6.1 expone los resultados de ejecutar las tareas formuladas por el MARA que, de acuerdo con el mapeo ilustrado por la Tabla 6.1, lograron satisfacer las actividades y entregables definidos por la fase 4 del proceso de planeación de un SGSI. A medida que se ejercita la adaptación propuesta se logra evaluar su desempeño como mecanismo para la gestión de riesgos, permitiendo identificar algunas fallas en su formulación, las cuales son expuestas por la sección 6.2. De esta manera se logra dar cumplimiento al segundo objetivo específico del proyecto. Luego, con base en las fallas identificadas por la sección 6.2, se ajusta la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, cumpliendo, así, el tercer objetivo específico. Finalmente, cabe mencionar que los autores de [64] proponen el uso de las encuestas como solución a la poca validación empírica de los estudios relacionados con las ciencias de la computación. En razón de lo expuesto y para reforzar la validación de la adaptación propuesta, se realiza: • una encuesta a dos expertos para evaluar el desempeño de la adaptación. • una encuesta de satisfacción al cliente destinada al jefe de la División de Gestión de Investigación quien, en su calidad de responsable de la ejecución del caso de estudio, termina siendo el usuario final de la solución construida. Dicha encuesta es tratada por la sección 6.3.	Cumplimiento total del segundo y tercer objetivo específico. Termina de cumplir el primer objetivo específico al ejecutar la cuarta y última fase del proceso de planeación de un SGSI, ilustrado por la Figura 2.2.

Tabla 1.1. Desarrollo del proyecto según [25]

Cabe mencionar que la revisión de la literatura permitió identificar dos estudios observacionales [67, 68] que fueron ejecutados sobre dos empresas de desarrollo de Software. Como este proyecto también se trata de un estudio observacional que se aplica sobre una organización en particular, se consideró de vital importancia complementar la metodología de desarrollo, especificada anteriormente, con las orientaciones impartidas por [67, 68].

Los autores de [68] afirman que el mayor obstáculo al que se enfrentaron, cuando intentaron conducir su estudio observacional, fue determinar un método apropiado para recolectar información, pues sus observaciones tenían que causar la menor interferencia posible en las actividades del personal estudiado. Respecto a lo anterior, en [63] se declara que, antes de dar inicio con las actividades, se debe decidir qué información recolectar y definir una manera apropiada de hacerlo.

- ¿Qué información recolectar?
  Para el presente estudio observacional resulta necesario recolectar toda la información requerida por las cuatro etapas de desarrollo del proyecto, descritas anteriormente por la Tabla 1.1.

- ¿Cómo recolectar la información?
  En [63] se afirma que los métodos de recolección de información pueden incluir: cuestionarios, observaciones, análisis de documentos, etc. Los autores de [67, 68] coinciden en un enfoque para la conducción de estudios observacionales que, en esencia, sugiere usar una combinación de entrevistas y observación de actividades para presentar una vista multidimensional del comportamiento estudiado, pues según [68], usar diferentes métodos para la recolección de datos ayuda a corroborar la evidencia y a identificar información adicional que no puede ser deducida desde la simple observación.

En virtud de lo señalado, durante el desarrollo del presente proyecto, se utiliza la observación y el análisis de documentos como métodos primarios para la recolección de información. Luego, por recomendación de [67], se realizan, cada que sea posible, algunas entrevistas y encuestas dirigidas al personal con el fin de validar las evidencias encontradas mediante la observación. Además, por recomendación de [68], las entrevistas se encuentran soportadas con grabaciones de audio.

Finalmente, en [68] se declara que uno de los retos asociados con la recolección de datos en estudios observacionales radica en la habilidad de registrar grandes cantidades de datos en tiempo real. Consecuentemente, se decide usar *FormStack* [75] para realizar encuestas en línea, lo cual permite indagar, simultáneamente, a todo el personal vinculado al caso de estudio sin causar interferencia alguna a sus labores diarias y brindando la flexibilidad y comodidad de responder desde cualquier lugar y en cualquier momento. Por recomendación de [68], toda la información obtenida es almacenada, procesada y analizada mediante el uso de programas ofimáticos como Microsoft Word [74] y Microsoft Excel [73]. Las evidencias de las entrevistas y

encuestas, celebradas en el marco del presente proyecto, se encuentran disponibles en [92].

1.8. Organización del documento

El presente documento se estructura de la siguiente manera:

- El capítulo 2 está destinado a la presentación del marco teórico.
- Los capítulos 3, 4, 5 y 6 abordan cada una de las cuatro etapas de desarrollo del proyecto de acuerdo con lo establecido por la sección 1.7.
- Conclusiones
- Bibliografía
- Anexos

1.8.1. Marco teórico

Como se mencionó anteriormente, el marco teórico es desarrollado por el capítulo 2 y su propósito es brindar, al lector, el conocimiento mínimo necesario que se requiere para comprender el problema del presente proyecto: ¿cómo adaptar la metodología MAGERIT V3 para lograr gestionar los riesgos de la SI en el caso de estudio? El marco teórico tratará los siguientes temas: *Gestión de riesgos de la SI, Proceso de planeación de un SGSI* y *Gestión de riesgos de la SI usando MAGERIT V3*.

1.8.2. Desarrollo del proyecto

De acuerdo con lo discutido por la sección 1.7, el desarrollo del proyecto se estructura en 4 etapas: estudio de pre-factibilidad, formulación del proyecto, ejecución del proyecto y validación de la solución, cada una de las cuales es abordada, respectivamente, por los capítulos 3, 4, 5 y 6, tal y como se describe a continuación:

- El capítulo 3 trata la primera etapa de desarrollo del proyecto: *Estudio de pre-factibilidad,* cuyo propósito es analizar el dominio del problema y determinar si se puede continuar con el proyecto. De acuerdo con lo establecido por la sección 1.7, en este capítulo se aborda la primera fase del proceso de planeación de un SGSI ilustrado por la Figura 2.2.

- El capítulo 4 trata la segunda etapa de desarrollo del proyecto: *Formulación del proyecto,* cuyo propósito es analizar los aspectos esenciales relacionados con la construcción de la solución y el aseguramiento de su viabilidad. De acuerdo

con lo establecido por la sección 1.7, en este capítulo se aborda las fases 2 y 3 del proceso de planeación de un SGSI expuesto por la Figura 2.2.

- El capítulo 5 trata la tercera etapa de desarrollo del proyecto: *Ejecución del proyecto,* cuyo propósito es construir la solución del proyecto. Cabe recordar que la solución al problema estudiado por el presente trabajo es: *"la adaptación de la metodología MAGERIT V3 como mecanismo para la gestión de los riesgos de la SI en procedimientos, que como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca"*

- El capítulo 6 trata la cuarta etapa de desarrollo del proyecto: *Validación de la solución,* cuyo propósito es ejercitar la solución y corregir los errores que se detecten. De acuerdo con lo establecido por la sección 1.7, en este capítulo se evidencia el uso de la adaptación con el fin de ejecutar la fase 4 del proceso de planeación de un SGSI, con lo cual se logra identificar y corregir cualquier deficiencia en su formulación. De igual manera, este capítulo evidencia cómo la adaptación propuesta es evaluada por expertos y, finalmente, sometida a una encuesta de satisfacción al usuario encaminada a reforzar la validación de la adaptación.

1.8.3. Anexos

Anexo A: Políticas de la SI para el caso de estudio.
En este anexo se define un completo conjunto de políticas encaminadas a brindar soporte y orientación a la gestión de la SI en el caso de estudio.

- **Anexo B: *Plantilla genérica de seguridad*.**

  En este anexo se expone la guía para la implementación de la plantilla genérica como un mecanismo para la comunicación de problemas e incidentes de la SI.

- ***Anexo C: Resultados de la gestión del riesgo***

  En este anexo se exponen los resultados de usar el MARA, producto de las adaptaciones a la metodología MAGERIT V3, para llevar a cabo la ejecución de la cuarta fase del proceso de planeación de un SGSI.

- ***Anexo D: Evaluación de la solución.***

  En este anexo se exponen las evidencias de las actividades de evaluación a las que fue sometida la adaptación propuesta

Capitulo 2

Marco Teórico

2.1. Gestión de riesgos de la SI

Actualmente, las organizaciones, sin importar su tipo o tamaño, necesitan de sus activos de información para funcionar correctamente y alcanzar sus metas. Los activos de información se caracterizan por ser susceptibles a ataques, errores y vulnerabilidades inherentes a su uso, exponiendo a la organización a un nivel de riesgo que puede afectar la consecución de los objetivos propuestos por la dirección. Por lo anterior, resulta esencial proteger los activos de información a través de la implementación, operación, y mejoramiento de la SI, haciendo posible que la organización cumpla su misión, mantenga el cumplimiento de sus obligaciones legales y mejore su reputación.

Según [16, 17, 18] la SI contempla 3 dimensiones primarias para cada activo de información: **confidencialidad**, **disponibilidad** e **integridad.** Para proteger estas dimensiones, la SI involucra la implementación y gestión de las medidas necesarias para garantizar la continuidad del negocio y minimizar el impacto causado por el amplio rango de amenazas que somete a las organizaciones. Ahora bien, para lograr la SI, se debe implementar un conjunto apropiado de controles que serán seleccionados a través de un proceso formal para la gestión de riesgos.

La gestión de riesgos de la SI es un enfoque sistemático que busca identificar las necesidades de la organización con respecto a los requerimientos de la SI. Con el fin de reducir el riesgo hasta niveles aceptables, este enfoque analiza lo que puede suceder y las consecuencias que de ello se deriven, antes de decidir lo que se debería hacer y cuando hacerlo. Generalmente, la gestión de riesgos de la SI debería contribuir a la:

- Identificación de los riesgos de la SI.

- Estimación de los riesgos en función del impacto que causa a la organización y la probabilidad de su ocurrencia.
- Definición del orden, por prioridad, del tratamiento de los riesgos.
- Educación, de los directores y el personal en general, acerca de los riesgos y las acciones que se deben tomar para mitigarlos.
- Participación de los interesados en la toma de decisiones.
- Comunicación y entendimiento de los resultados de las acciones tomadas para mitigar los riesgos.
- Revisión y monitoreo del riesgo.

De acuerdo con las conclusiones del estado del arte, para poder gestionar los riesgos de la SI en el caso de estudio, se deberá abordar las fases comprendidas por el proceso de planeación de un SGSI.

2.2. Proceso de planeación de un SGSI

Como se mencionó en la sección 1.4, el estándar ISO/IEC 27003 [4] provee una guía práctica para llevar a cabo la planeación del SGSI de acuerdo con los requerimientos de la norma ISO/IEC 27001 [2]. Para ello, el estándar ISO/IEC 27003 propone el proceso ilustrado por la Figura 2.2, en el cual se identifican las fases y actividades que se deberán abordar. Se debe recordar que, por recomendación del Foro de Implementación ISO27k, el *Diseño del SGSI* no será parte de la planeación del SGSI[20].

A continuación, la Figura 2.1 muestra la simbología que usará la Figura 2.2 para ilustrar el proceso de planeación de un SGSI. Luego, las secciones 2.2.1 a la 2.2.4 describirán cada una de las fases definidas por dicho proceso.

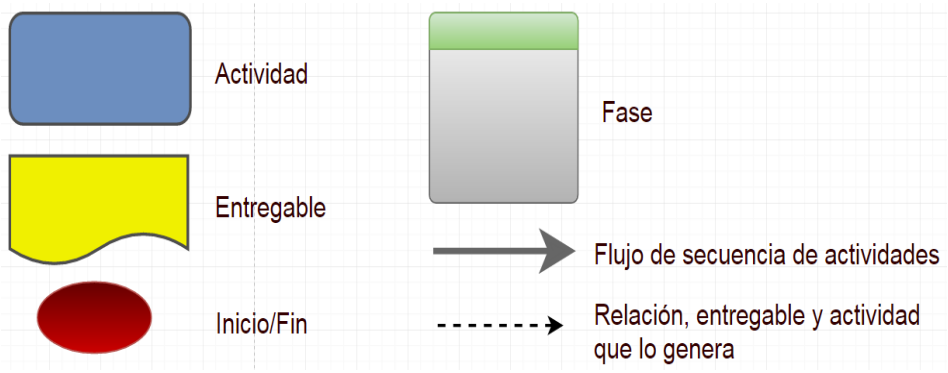

Figura 2.1. Simbología del proceso de planeación de un SGSI. Fuente: propia de los autores

[20] Para mayor información, retomar la sección 1.4.

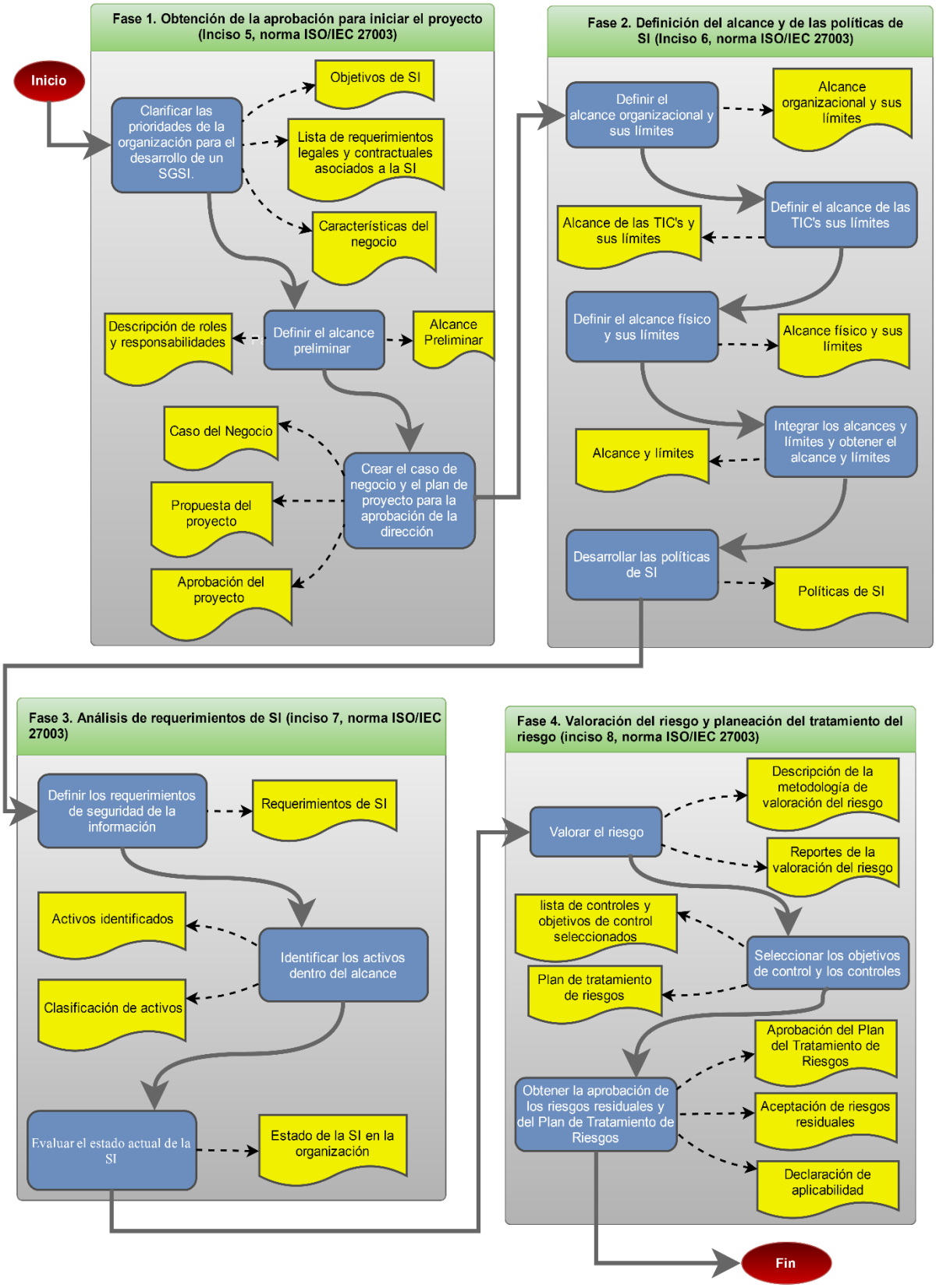

Figura 2.2. Proceso de planeación de un SGSI. Tomada de [4]

2.2.1. Fase 1: Obtención de la aprobación para iniciar el proyecto.

El objetivo de esta fase es dar a conocer la importancia de implementar el SGSI con el fin de obtener la aprobación y compromiso de la dirección para dar inicio al proyecto de implantación del SGSI.

2.2.2. Fase 2: Definición del alcance del SGSI y las políticas de SI.

- **Definición del alcance del SGSI.**

El alcance determina el esfuerzo requerido para implementar el SGSI, impactando todas las actividades relacionadas con la gestión de la SI, por ende, deberá ser cuidadosamente definido a fin de garantizar que todos los activos importantes se encuentren debidamente protegidos. Según el estándar ISO/IEC 27003 [4], el alcance del SGSI puede ser determinado integrando los alcances: organizacional, físico y de las TIC, los cuales, por recomendación de los autores de [12], pueden ser definidos usando la Metodología de las Elipses[21] propuesta en [13].

- **Definición de las políticas de la SI.**

Una política de la SI es un documento que provee directrices generales de alto nivel para brindar la orientación y el soporte necesario para lograr los objetivos de la implantación del SGSI. Mediante la política de la SI, la organización revela su postura con respecto a la protección de sus activos de información y a la implantación y soporte de su SGSI.

2.2.3. Fase 3: Análisis de requerimientos de SI

A partir del caso de negocio, esta fase busca analizar y definir, en detalle, los requerimientos que debe soportar el SGSI e identificar los activos de información con el fin de determinar el nivel de protección deseado, las vulnerabilidades y el estado actual de la SI. Para lograr lo anteriormente descrito, esta fase define las siguientes actividades:

- **Identificación de los activos cubiertos por el alcance del SGSI.**

Para abordar esta actividad conviene identificar de cada activo una breve descripción, cantidad y tipo.

- **Definición de los requerimientos para el SGSI.**

Para definir los requerimientos para el SGSI se debe considerar los activos de información, formas de procesamiento y gestión de la información, requerimientos legales, obligaciones contractuales y los niveles de conocimiento y conciencia, que posee el personal, en materia de la SI.

[21] La recomendación de los autores de [12] se acoge debido a la similitud de su trabajo con el presente proyecto.

❖ **Evaluación del estado actual de la SI.**

El propósito de esta actividad es identificar un esbozo del estado actual de la SI y describir las vulnerabilidades que, en conjunto con los objetivos del SGSI, buscarán incentivar la SI.

2.2.4. Fase 4: Valoración del riesgo y planeación del tratamiento

El estándar ISO/IEC 27005 [5] propone abordar dichos aspectos mediante un proceso formal para la gestión de riesgo de la SI, ilustrado por la Figura 2.3, el cual analiza lo que puede suceder y sus posibles consecuencias, antes de tomar decisiones sobre qué hacer, para lograr, de esta manera, reducir el riesgo hasta un nivel aceptable. El estándar ISO/IEC 27005 [5], en su Tabla 1, declara que en un SGSI, cuya implementación se base en el modelo PDCA, las actividades del proceso de gestión de riesgos que corresponden a la planeación de un SGSI y que, por ende, se deben abordar por el presente proyecto, son: establecimiento del contexto, valoración del riesgo, desarrollo del plan de tratamiento del riesgo y aceptación del riesgo.

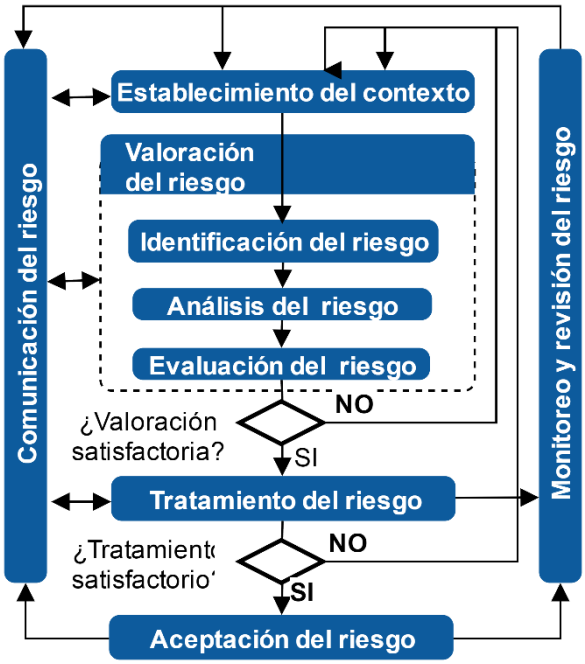

Figura 2.3. Proceso de gestión de riesgos. Tomado de [5]

❖ **Establecimiento del contexto.**

Según el estándar ISO/IEC 27005, entender y establecer el contexto de la organización garantiza, en gran parte, que el proceso de gestión de riesgos será un enfoque adecuado, preciso y confiable. Esto implica definir los criterios básicos y la organización necesaria para operar la gestión del riesgo.

❖ **Valoración del riesgo.**

Según el estándar ISO/IEC 27005, la valoración del riesgo pretende identificar, cuantificar y priorizar los riesgos de la SI. Para ello, resulta necesario:

- Identificar el riesgo. El objetivo de esta actividad es determinar todo aquello que pueda causar pérdidas potenciales a la organización, para lo cual se deberá identificar: los activos relevantes dentro del alcance, las amenazas que atentan contra dichos activos, las vulnerabilidades de la organización y las consecuencias de la materialización de dichas amenazas.

- Analizar el riesgo con el propósito de describir y cuantificar la magnitud potencial de las consecuencias y su probabilidad de ocurrencia. En [22] se propone una serie de pasos para abordar esta actividad como se muestran a continuación:

    1. Valorar los activos identificados.

    2. Valorar las amenazas identificadas. De una amenaza conviene estimar su influencia sobre el valor de los activos, para lo cual, se debe determinar la probabilidad de ocurrencia y la degradación que causa como la **fracción del valor** que se pierde del activo[22].

    3. Estimar el impacto sufrido por los activos a raíz de la degradación causada por las amenazas identificadas. El impacto se expresa como **el valor que pierde** el activo[23] y es determinado, por cada amenaza, con la siguiente ecuación:

    $$\boldsymbol{I = V * D}$$

    Donde, V es el valor del activo y D es la degradación o fracción del valor que pierde el activo si la determinada amenaza se llega a materializar.

    4. Estimar el riesgo de que cada amenaza se materialice sobre los activos, causando pérdidas y perjuicios para la organización. Su cálculo se puede llevar a cabo con la siguiente ecuación:

    $$\boldsymbol{R = I * P}$$

    Donde, I es el impacto que sufriría un activo si una determinada amenaza se llegara a materializar y P la probabilidad de materialización de dicha amenaza.

Los conceptos tratados anteriormente, sobre el análisis de riesgos, son ilustrados, a continuación, por la Figura 2.4.

[22] Por ejemplo, la amenaza fuego puede degradar en un 90% el valor de los activos.
[23] Por ejemplo, si la amenaza fuego, que puede causar una degradación del 90%, se materializa sobre un activo que vale $100’000.000, entonces el impacto será de $90’000.000

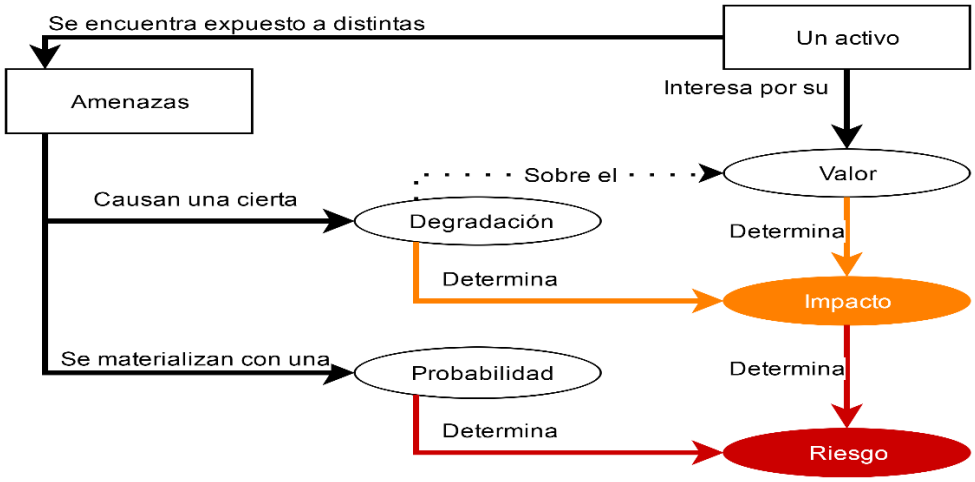

Figura 2.4. Conceptos sobre el análisis de riesgos. Tomada de [22]

- Evaluación del riesgo. El objetivo de esta actividad es priorizar los riesgos identificados y analizados anteriormente, clasificándolos mediante la aplicación de los criterios para la evaluación del riesgo que se han de definir durante el establecimiento del contexto. De esta manera, se usa el conocimiento adquirido del análisis de riesgos para tomar decisiones sobre acciones futuras[24]. Finalmente, se obtendrá la lista de prioridades para el tratamiento que se describe a continuación.

❖ **Tratamiento del riesgo.**

Según el estándar ISO/IEC 27005 [5], hay cuatro opciones disponibles para tratar los riesgos de la SI: modificación, retención, evitación y transferencia.

OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN
Modificación del riesgo	El nivel del riesgo debería ser gestionado mediante introducción, remoción o alteración de controles.
Retención del riesgo	Si el nivel del riesgo satisface los criterios para su aceptación, no será necesario implementar controles y el riesgo se puede retener.
Evitación del riesgo	Cuando los riesgos se consideren muy altos o si el costo de implementar el tratamiento excede los beneficios, se puede tomar la decisión de evitar el riesgo mediante el retiro de la actividad o activo, cambiando las condiciones bajo las cuales se ejecuta la actividad o adecuando el entorno donde se encuentran los activos involucrados.

[24] Como, por ejemplo: ¿se debe tratar este riesgo?, ¿qué riesgos se deben tratar primero?, ¿cuál es la prioridad?

Transferencia del riesgo	El riesgo se debería transferir a otra parte que cuente con la capacidad de gestionar de manera más eficaz el riesgo en cuestión.

Tabla 2.1. Opciones de tratamiento. Tomada de [5]

El propósito de esta actividad es, con base en los criterios para el tratamiento de riesgos y la lista de prioridades obtenida anteriormente, seleccionar las opciones de tratamiento con las cuales se buscará mitigar cada riesgo identificado. Como resultado se obtendrá el Plan de Tratamiento del Riesgo. Luego, será necesario determinar los riesgos residuales, lo cual implica una actualización de la valoración del riesgo, considerando los efectos esperados de los controles seleccionados.

- **Aceptación del Riesgo.**

El propósito de esta actividad es tomar la decisión de aprobar, o no, los riesgos residuales estimados anteriormente. Los que no sean aprobados pueden ser objeto de nuevas iteraciones del tratamiento hasta que cumplan los criterios de aceptación. Una vez se hayan aceptado los riesgos residuales, se debe desarrollar la Declaración de Aplicabilidad donde se relacionen los controles y objetivos de control que fueron seleccionados para tratar los riesgos de la SI, justificando claramente las razones de las inclusiones y exclusiones de los controles sugeridos por el anexo A de la norma ISO/IEC 27001 [2].

Por todo lo anterior, resulta evidente que el estándar ISO/IEC 27005 [5] provee las directrices para gestionar el riesgo, sin embargo, éste no define ninguna metodología específica para tal fin. Como se mencionó en el capítulo 1, para el presente proyecto se decide probar con MAGERIT V3. Dicha selección se encuentra debidamente justificada por la revisión del estado del arte que se encuentra disponible en la sección 1.4.

Ya habiendo justificado la elección de la metodología, la siguiente sección del marco teórico se encargará de tratar las generalidades de MAGERIT V3 y del enfoque que ésta propone para abordar las actividades de la gestión de riesgos pertinentes a la planeación del SGSI. De este modo, se logra satisfacer el entregable *Descripción de la metodología de valoración del riesgo,* requerido por la cuarta fase del proceso de planeación de un SGSI[25].

[25] Ver Figura 2.2. *Proceso de planeación de un SGSI*

2.3. Gestión de riesgos de la SI usando MAGERIT V3

MAGERIT V3 es una reconocida metodología que implementa el proceso de gestión de riesgos definido por el estándar ISO/IEC 27005[26]. Elaborada por el Consejo Superior de Administración Electrónica de España en respuesta a la creciente dependencia que tiene la sociedad hacia las tecnologías de la información y las comunicaciones. Para implementar el proceso de gestión de riesgos dictado por el estándar ISO/IEC 27005, MAGERIT V3 persigue una aproximación metódica que no deje lugar a la improvisación ni dependa de la arbitrariedad del analista, ofreciendo un método sistemático que, según [24], puede acudir a dos posibles técnicas para la valoración y tratamiento del riesgo: el uso de tablas o el análisis algorítmico, el cual, a su vez, ofrece dos enfoques: cualitativo y cuantitativo. En la sección 5.3.8 se brindan las orientaciones relacionadas con la selección de la técnica para la valoración y el tratamiento del riesgo.

A continuación se identifican las tareas y demás disposiciones que MAGERIT V3 formaliza en [22] con el fin de cubrir cada una de las actividades del proceso de gestión del riesgo que deben ser ejecutadas durante la planeación del SGSI.

2.3.1. Establecimiento del contexto con MAGERIT V3.

Según el estándar ISO/IEC 27005, el enfoque definido para la gestión de riesgos debería ser adecuado para el entorno de la organización y parte integral de todas sus actividades asociadas con la SI. Por ende, resulta de vital importancia que, antes de aplicar la metodología MAGERIT V3, ésta sea adaptada al contexto del caso de estudio, lo cual implicará definir, como se mencionó en la sección 2.2.4:

- Los criterios para la evaluación y tratamiento del riesgo, así como para la valoración de activos, amenazas y salvaguardas, con el fin de obtener resultados reproducibles, comparables, objetivos e imparciales. MAGERIT V3 solamente define, en [23], un conjunto de criterios para valorar los activos que deberá ser adaptado al contexto del caso de estudio. Por tal motivo, en el capítulo 5 se discute la necesidad de agregar nuevas actividades a la metodología MAGERIT V3 para garantizar la definición de los criterios necesarios para una adecuada gestión de riesgos de la SI.

- La organización necesaria para operar la gestión del riesgo. Respecto a lo anterior, se encuentra que la definición de roles propuesta por MAGERIT V3 en [22], al no estar alineada con la estructura organizacional de la Universidad del Cauca y por no ser muy específica, da cabida a la ausencia, desentendimiento y evasión de las responsabilidades en materia de la gestión de riesgos de la SI. Por tal motivo, en

[26] Ver Figura 2.3. Proceso de gestión de riesgos.

el capítulo 5 se discute la necesidad de agregar una nueva actividad a la metodología MAGERIT V3 para garantizar la definición adecuada de los roles y responsabilidades.

2.3.2. Valoración y tratamiento del riesgo según MAGERIT V3.

En [22] se evidencia que, para abordar la valoración y el tratamiento de riesgos, la metodología MAGERIT V3 formaliza las siguientes actividades:

- **MAR.1. Caracterización de los activos.**

Según [22], esta actividad busca identificar los activos relevantes, caracterizándolos por su tipo, identificando sus dependencias, determinando en qué dimensiones son importantes y valorando esta importancia.

En [22], MAGERIT V3 declara que los activos esenciales son la información y los servicios. Estos dependen de otros activos más prosaicos como los equipos, las instalaciones, las redes de comunicaciones y las personas, entre otros. De esta manera, los activos van formando árboles, como el ilustrado, a continuación, por la Figura 2.5, que representan, de arriba hacia abajo, las dependencias y, de abajo hacia arriba, la propagación del daño hasta los activos superiores en caso de materializarse una amenaza sobre un activo inferior.

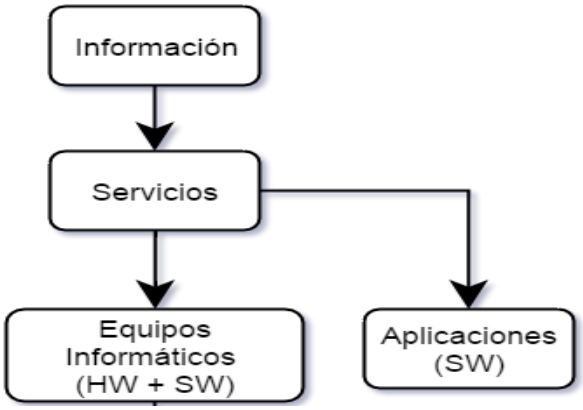

Figura 2.5. Ejemplo de un árbol de dependencias. Tomada de [22]

Según [22], la importancia de identificar las dependencias radica en que por medio de éstas:

- se propaga el valor de los activos. Por ejemplo, con base en la Figura 2.5: si cierta información I es un activo extremadamente valioso y depende de un servicio S, sabemos que cualquier daño sobre S se propagará hacia I. Por lo tanto, proteger a I implica resguardar a S, lo cual convierte a S en algo valioso que se debe proteger. De ese modo es como los activos inferiores heredan valor de sus superiores a través de las dependencias.

- se propaga el impacto. De la misma manera como ocurre con el valor, el impacto sufrido por un activo inferior, a causa de la materialización de una amenaza, se transmite a todos sus superiores, incrementando considerablemente el nivel de riesgo.

Consecuentemente, para caracterizar los activos, MAGERIT V3 define las siguientes sub-tareas:

- MAR.1.1. Identificación de los activos.
- MAR.1.2. Identificación de las dependencias entre activos.
- MAR.1.3. Valoración de los activos.

❖ **MAR.2. Caracterización de las amenazas.**

Según [22], esta actividad pretende identificar y valorar las amenazas que pueden afectar los activos de información, para lo cual MAGERIT V3 define las siguientes sub-tareas:

- MAR.2.1: Identificación de las amenazas
- MAR.2.2: Valoración de las amenazas.

❖ **MAR.3. Caracterización de salvaguardas.**

Según [22], esta actividad busca identificar los controles[27] ya implementados por el caso de estudio, sin embargo, la descripción de las sub-tareas, que en [22] se encuentra, revela que el verdadero objetivo es identificar y valorar los controles que se necesitan para proteger los activos y que aún no han sido implementados. Las sub-tareas, de las que se hacía mención, son las siguientes:

- MAR.3.1: Identificación de las salvaguardas pertinentes.
- MAR.3.2: Valoración de las salvaguardas.

De lo anterior se evidencia que este enfoque, propuesto por MAGERIT V3, pretende seleccionar los controles necesarios para tratar el riesgo sin antes haber estimado el riesgo mismo. Cabe mencionar que la norma ISO/IEC 27001 [2] define una serie de requisitos para la valoración y el tratamiento de riesgos de la SI, como los estipulados por las cláusulas 6.1.2 y 6.1.3, que establecen que la selección de los controles debe llevarse a cabo después de:

1. Identificar y analizar los riesgos (incluye la estimación de los niveles de riesgo).
2. Evaluar los riesgos para obtener una lista de prioridades para el tratamiento.

De esta manera, se logra identificar que la disposición de las actividades propuestas por MAGERIT V3, en [22], incumple los requerimientos establecidos por la norma ISO/IEC 27001 [2]. En el capítulo 5 se discuten las adaptaciones que fueron necesarias para corregir dicha desviación.

[27] Cabe recordar que, como se mencionó en el glosario de este documento, los términos "*salvaguarda"* y "*control"* son equivalentes y que, por ende, pueden ser usados indistintamente.

❖ **MAR.4. Estimación del estado de riesgo.**

Según [22], el objetivo de esta actividad es determinar el nivel de riesgo, al que se encuentra expuesta la organización, para lo cual será necesario abordar las siguientes sub-tareas:

- MAR.4.1: Estimación del impacto.
- MAR.4.2: Estimación del riesgo.

2.3.3. Aceptación del riesgo según MAGERIT V3.

En [22], MAGERIT V3 manifiesta que la Dirección de la organización sometida a la gestión de riesgos debe determinar el nivel de impacto y riesgo aceptable, asumiendo la responsabilidad de las insuficiencias. Claramente esta decisión no es técnica, sino más bien, una decisión política o gerencial que puede venir determinada por las leyes o por compromisos contractuales con terceras partes. En consecuencia, cualquier nivel de impacto y/o riesgo será considerado aceptable si, y sólo sí, es conocido y aprobado formalmente por la Dirección. En el capítulo 5 se discute la necesidad de agregar una nueva actividad a MAGERIT V3 que permita formalizar la aceptación de los riesgos.

Capitulo 3

Estudio de pre-factibilidad

Durante esta primera etapa de desarrollo del proyecto se pretende analizar el dominio del problema[28] y determinar si se puede continuar con el proyecto. El análisis del dominio del problema fue llevado a cabo mediante la ejecución de las actividades de la primera fase del proceso de planeación de un SGSI expuesto por la Figura 2.2.

La ejecución de las actividades de la primera fase del proceso de planeación de un SGSI: *Obtener aprobación para iniciar el proyecto*, dejó como resultado:

- El caso de negocio, mediante el cual se logró analizar el dominio del problema gracias a la identificación de las características, prioridades y requerimientos del caso de estudio en materia de la SI. De acuerdo con lo establecido por el estándar ISO/IEC 27003 [4], este documento también incluye: los objetivos de SI, un cronograma de actividades, el alcance preliminar, presupuesto y los roles y responsabilidades relacionados con el proyecto.

  El caso de estudio es abordado por la sección 3.1, logrando, de esa manera, analizar el dominio del problema y satisfacer los primeros seis entregables requeridos por la fase 1 del proceso de planeación de un SGSI.

- La aprobación del proyecto.

[28] ¿Cómo adaptar la metodología MAGERIT V3 para lograr gestionar los riesgos de la SI en el caso de estudio?

3.1. Caso de negocio

Los autores de [66] declaran que es extremadamente importante que los estudios observacionales reporten gran cantidad de información contextual con el fin de garantizar que los resultados que se obtengan sean entendidos adecuadamente. Debido a ello, con las siguientes secciones, que describen el *Caso de Negocio,* se pretenderá esclarecer, con el mayor nivel de detalle posible, todas las características y particularidades del caso de estudio y su contexto.

3.1.1. Características del negocio[29].

- **Estructura de procesos y procedimientos de la Universidad del Cauca.**

La dirección de la Universidad del Cauca, como institución de educación superior comprometida con la calidad, formación, investigación y la interacción social, pretende garantizar la excelencia como criterio orientador para la mejora continua de los procesos institucionales. En virtud de lo señalado, la administración universitaria, acogiendo la ley 872 de 2003[30] [26], decide adoptar el Sistema Integrado de Gestión de Calidad en la Universidad del Cauca[31] como herramienta que permita dirigir y evaluar el desempeño institucional en términos de calidad y satisfacción en la prestación de servicios. Dicho sistema involucra los requerimientos estipulados por la norma técnica de calidad en la gestión pública NTCGP1000 [27] y el Modelo Estándar de Control Interno para el estado colombiano [28].

En relación con el Sistema Integrado de Gestión de Calidad, en la Universidad del Cauca se han adelantado acciones tendientes al mejoramiento institucional a través de varios actos administrativos como, por ejemplo, la resolución R-220 de 2011, por la cual se adopta el Manual de Calidad que se encuentra especificado por el documento PE-GS-2.2.1-MN-1 [30], en el cual se define el mapa de procesos del alma máter que se ilustra, a continuación, por la Figura 3.1.

[29] El término *negocio,* usado por el estándar ISO/IEC 27003 [4], hace referencia al caso de estudio.
[30] Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios.
[31] Reglamentado por la Resolución R-802 de 2011 [29]

Figura 3.1. Mapa de procesos de la Universidad del Cauca. Tomada de [30]

- **Procesos Estratégicos:** establecen las políticas, directrices y estrategias en la Universidad del Cauca, para el cumplimiento de la misión.

- **Procesos Misionales:** ejecutan las directrices en cumplimiento de las normas para la satisfacción de la parte interesada.

- **Procesos de Apoyo:** proveen los recursos e insumos necesarios para el funcionamiento articulado con todos los procesos del sistema.

- **Procesos de Evaluación:** controlan, evalúan y hacen seguimiento a la gestión en todos los procesos universitarios.

❖ **Descripción del caso de estudio**

El Proceso Misional: Gestión de la Investigación, especificado por el documento PM-IV-6-CA [31], tiene por objetivo propiciar y generar condiciones para la creación y el fortalecimiento de los grupos de investigación de la Universidad del Cauca. Este proceso está soportado por los siguientes procedimientos:

- Creación y registro de grupos de investigación
- Formulación y ejecución de proyectos de investigación de desarrollo interno
- Formulación y ejecución de proyectos con financiación externa
- Participación en convocatorias internas de proyectos de investigación y su ejecución
- Aplicación a programas de apoyo de la Vicerrectoría de Investigaciones
- Homologación de materias con trabajos de proyectos de investigación

Para el presente proyecto, se ha elegido como caso de estudio la *Formulación y ejecución de proyectos con financiación externa*, especificado por el documento PM-IV-6.1-PR-3 [32]. Este procedimiento tiene por objetivo, coordinar la presentación y ejecución de proyectos de investigación con financiación externa, orientando a los grupos de investigación sobre los trámites, compromisos y/o requisitos para acceder a la cofinanciación de entidades externas

Como se mencionó en el capítulo 1, el caso de estudio es considerado un procedimiento crítico de la Universidad del Cauca, justificando, de esa manera, la necesidad de proteger sus activos de información en las tres dimensiones primarias: confidencialidad, integridad y disponibilidad.

A continuación, las Figuras 3.3, 3.4, 3.5 y 3.6 ilustrarán el diagrama de flujo del caso de estudio con base en la simbología descrita por la Figura 3.2

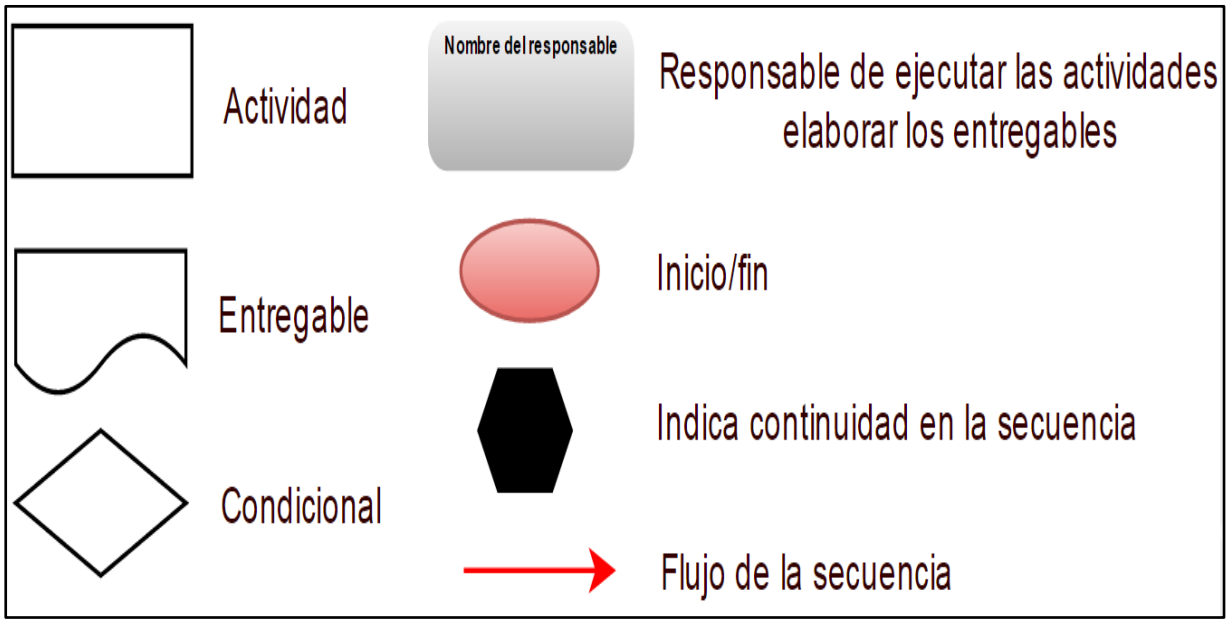

Figura 3.2. Simbología del diagrama de flujo del caso de estudio.
Fuente: propia de los autores

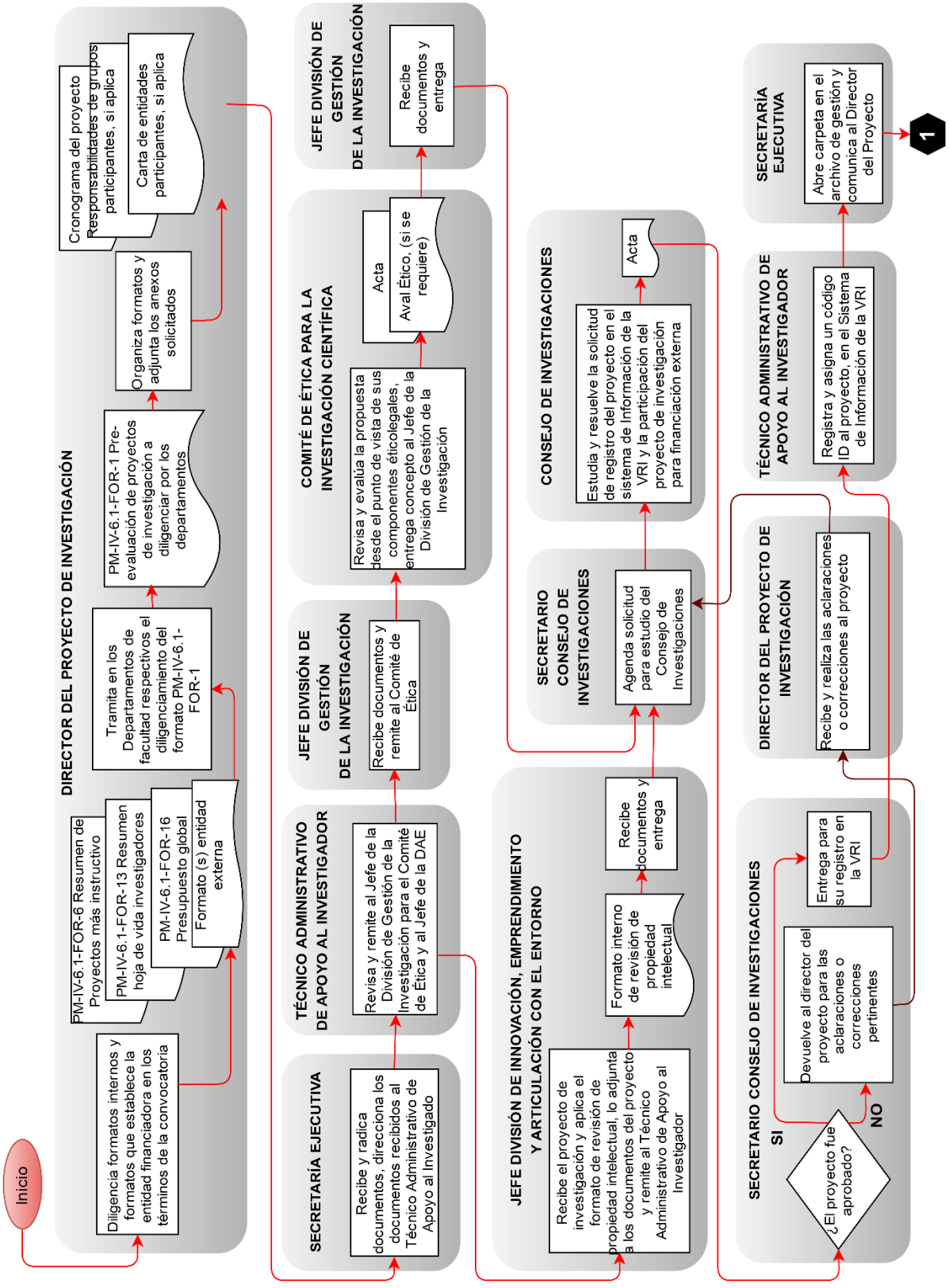

Figura 3.3. Diagrama de flujo del caso de estudio. Parte I. Tomada de [32]

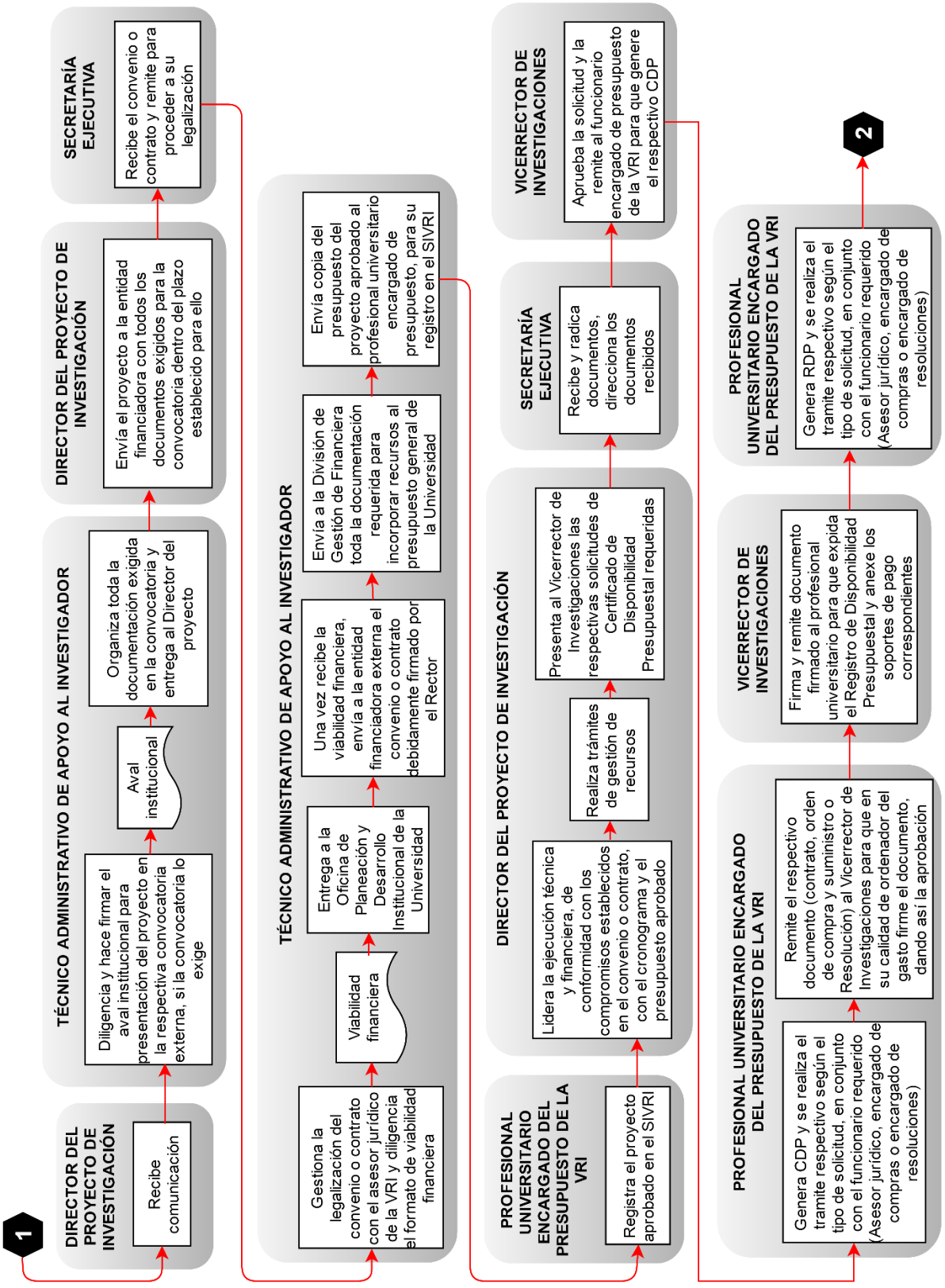

Figura 3.4. Diagrama de flujo del caso de estudio. Parte II. Tomada de [32]

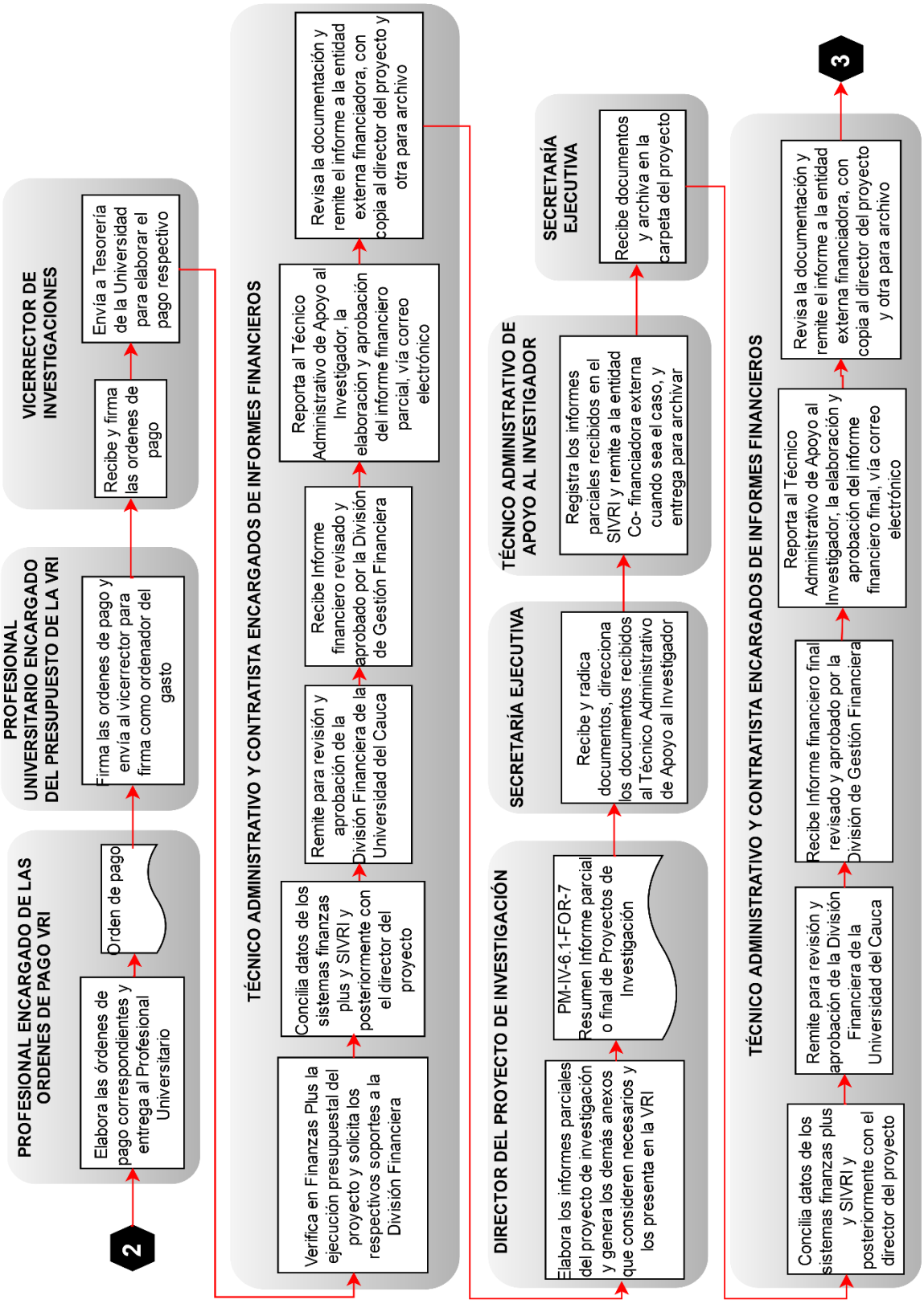

Figura 3.5. Diagrama de flujo del caso de estudio. Parte III. Tomada de [32]

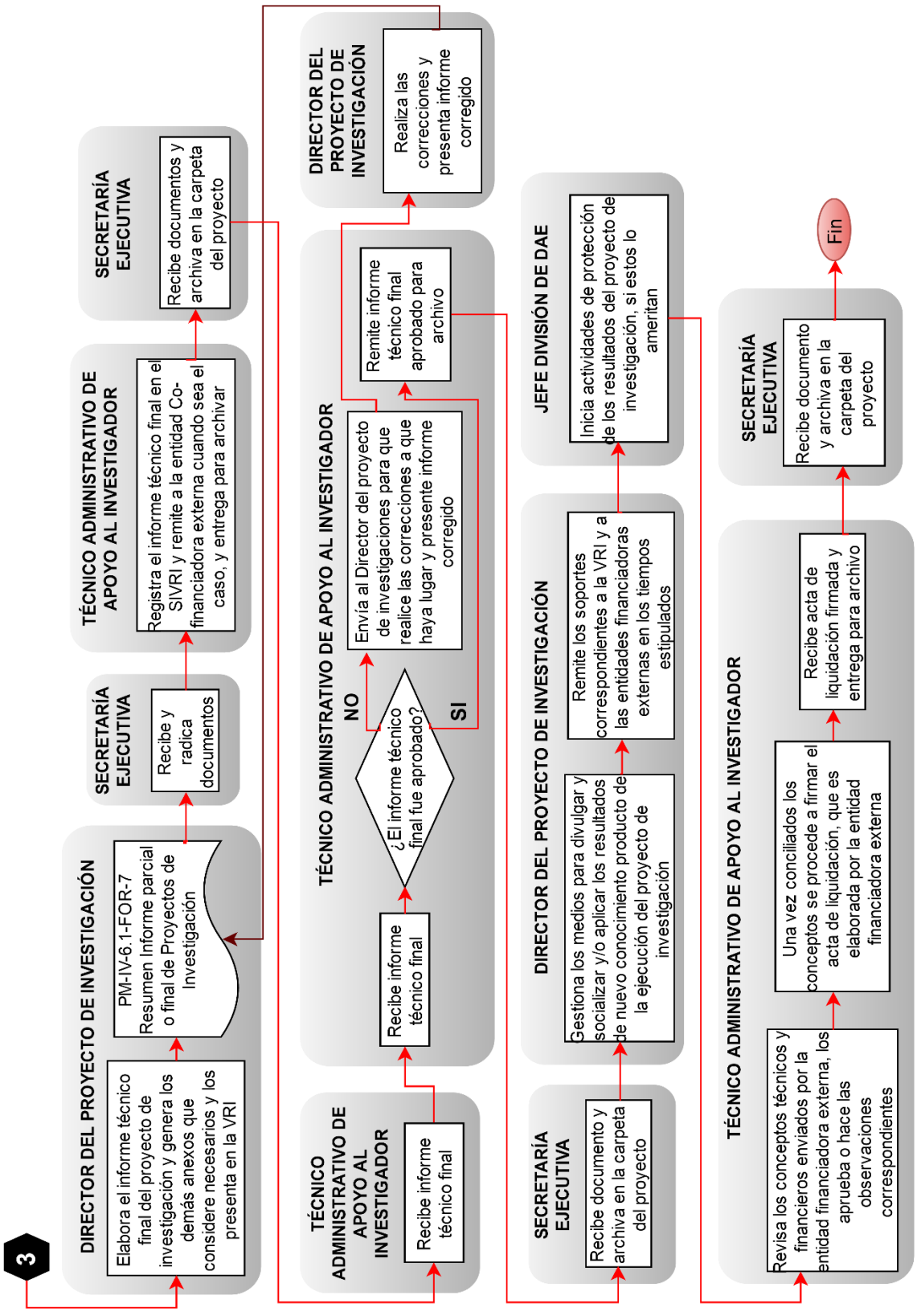

Figura 3.6. Diagrama de flujo del caso de estudio. Parte IV. Tomada de [32]

3.1.2. Prioridades del caso de estudio en materia de la SI.

El caso de estudio, como componente de uno de los procesos misionales de la Universidad del Cauca, adquiere la obligación de observar y cumplir lo estipulado por la política del SGSI de la institución [34]. Por ende, una de las prioridades del caso de estudio debe ser soportar y contribuir al logro de los objetivos de la SI que se ha propuesto el alma mater en el artículo primero de la política de su SGSI. A continuación se da a conocer el conjunto de necesidades preponderantes del caso de estudio.

a. Proteger los activos de información involucrados en las actividades del caso de estudio, minimizando el riesgo de la SI al que se encuentran expuestos.
b. Garantizar el cumplimiento de las obligaciones contractuales con entidades externas con el fin de evitar consecuencias legales y económicas derivadas de cualquier incumplimiento.
c. Mantener la confianza que la comunidad investigadora y las entidades externas que financian los proyectos de investigación, tienen hacia el caso de estudio, otorgándoles la garantía de que los activos de información están protegidos adecuadamente.
d. Contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, entregando, como aporte, la gestión de riesgos en un procedimiento crítico de la institución.

3.1.3. Requerimientos legales, regulatorios y contractuales.

En materia de la SI, las leyes y decretos que pueden intervenir en las operaciones del caso de estudio, son:

- Ley 527 de 1999 [35]: por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley estatutaria 1266 de 2008 [36]: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley estatutaria 1581 de 2012 [37]: por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013 [38]: Por el cual se reglamenta parcialmente la ley 1581 de 2012.

En el desarrollo pleno de sus actividades, el caso de estudio se ve involucrado en la recolección, almacenamiento, uso, circulación o supresión de datos personales, otorgándole a la VRI, por disposición de la ley 1581 de 2012 [37] y del decreto 1377

de 2013 [38], la calidad tanto de Responsable del Tratamiento como de Encargado del Tratamiento de datos personales. Como consecuencia, la VRI adquiere todas las responsabilidades y deberes que de ello derivan:

a. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data. En consecuencia, adquiere el deber de observar y cumplir las disposiciones de la ley 1266 de 2008.
b. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
c. Observar y aplicar las demás disposiciones de la ley estatutaria 1581 de 2012 y su Decreto Reglamentario 1377 de 2013.

Por otra parte, el caso de estudio deberá acoger lo estipulado por la ley 527 de 1999. A continuación se listan algunos requerimientos emanados por dicha ley.

a. Se debe reconocer la firma digital como un elemento jurídico que tiene la misma fuerza y efectos que la firma manuscrita, siempre y cuando incorpore los atributos jurídicos establecidos por el artículo 28 de la ley 527 de 1999:
b. Obtener las firmas digitales acudiendo solamente a entidades que estén acreditadas por el Organismo Nacional de Acreditación conforme a la reglamentación expedida por el Gobierno Nacional[32].

Adicionalmente, el caso de estudio deberá contemplar el cumplimiento de las obligaciones que la VRI adquiere por la celebración de contratos y convenios con entidades financiadoras, personas naturales o jurídicas y demás terceros vinculados. A los requisitos imputados por las contrapartes de los contratos o convenios, se le suman las siguientes exigencias del Estatuto de Contratación de la Universidad del Cauca [39], en materia de la SI:

a. Los contratos celebrados con entidades del exterior y que se ejecuten en Colombia, deben regirse por las leyes colombianas. Y los celebrados con entidades del exterior y que deban ejecutarse en el exterior podrán regirse por las normas del respectivo país.
b. Examinar los elementos constitutivos del contrato a celebrar, tales como los sujetos, el objeto, la capacidad y la pertinencia institucional.
c. Designar interventores o supervisores para que se ejerza una adecuada vigilancia durante la ejecución de los contratos y el cumplimiento de los mismos.
d. Tramitar las solicitudes de ingreso del personal y equipo del contratista o de personas externas a las áreas de influencia del contrato.

[32] Artículo 160 del Decreto Nacional 019 de 2012, mediante el cual se modifica el artículo 29 de la ley 527 DE 1999 (agosto 18, Colombia).

3.1.4. Objetivos de SI

Con el fin de dar apoyo a la iniciativa de la Universidad del Cauca en materia de la SI y reducir el nivel de riesgo al que se encuentra sometido el caso de estudio, la implantación del SGSI perseguirá los siguientes objetivos:

- Definir e implementar políticas y procedimientos para la gestión de la SI en el caso de estudio.
- Valorar y tratar los riesgos de la SI en el caso de estudio.
- Obtener conformidad legal frente a la normativa colombiana, asociada con la SI, como la ley para la protección de datos personales y su decreto reglamentario.
- Garantizar el cumplimiento de las obligaciones contractuales con las entidades externas que financian los proyectos de investigación.
- Dar soporte al SGSI de la Universidad del Cauca.

3.1.5. Alcance preliminar.

Según el Acuerdo Superior 015 del 2015 [40], emitido por el Consejo Superior de la Universidad del Cauca, la VRI está integrada por varias unidades incluyendo la División de Gestión de Investigación que, por disposición del artículo 4.2 de éste acuerdo, tiene a su cargo la ejecución de los procedimientos que soportan el proceso misional: *Gestión de la Investigación*. Uno de ellos es el caso de estudio, el cual se ubica jerárquicamente en la estructura organizacional de la VRI tal y como lo muestra, a continuación, la Figura 3.7.

Figura 3.7. Estructura organizacional de la VRI. Fuente: propia

A manera preliminar, el alcance del SGSI incluirá toda actividad pertinente a la gestión de la SI, únicamente, para el caso de estudio y sus activos de información. También es de la incumbencia del SGSI garantizar que el caso de estudio satisfaga los requerimientos que adquiere de sus obligaciones contractuales con entidades externas y los emanados por la ley de protección de datos personales, hábeas data y demás leyes colombianas. Del alcance se excluye toda actividad ajena a la gestión de la SI y cualquier acción que involucre activos ajenos al caso de estudio.

3.1.6. Descripción de roles y responsabilidades

Considerando la estructura organizacional de la Universidad del Cauca, se define, a manera de propuesta, los siguientes roles y responsabilidades frente a las actividades de SI para el caso de estudio:

ROL	DESCRIPCIÓN	RESPONSABILIDADES
Comité de Dirección	Está conformado por: Rector, Vicerrector Administrativo, Vicerrector Académico, Vicerrector de Investigaciones, Vicerrector de Bienestar y Cultura, Jefe Oficina de Planeación	1. Aprobar los objetivos y planes del SGSI. 2. Aprobar las políticas, normas y procedimientos de la SI. 3. Asignar los recursos suficientes para el desarrollo, implementación, operación, auditorías y certificación del SGSI. **4.** Aprobar la estructura organizacional del SGSI, sus roles y responsabilidades. **5.** Aprobar los planes de capacitación y sensibilización de la comunidad académica relacionada con la SI.
Comité de la SI	Sus miembros son los encargados de velar por el correcto desempeño del SGSI desde la División de la Universidad que esté a su cargo y revisar minuciosamente cualquier documento del	1. Revisar las políticas, normas y procedimientos de la SI. 2. Establecer objetivos y planes del SGSI. 3. Establecer roles y responsabilidades de la SI. 4. Solicitar y ejecutar los recursos asignados. 5. Decidir los criterios de aceptación de riesgos y sus respectivos niveles. 6. Asegurar que se realicen periódicamente revisiones y auditorías internas. 7. Garantizar el establecimiento, implementación, operación, monitoreo,

	SGSI para su aprobación por el mismo Comité.	revisión, mantenimiento, mejoras, auditorías y certificación del SGSI. 8. Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad. 9. Velar por la correcta implementación de los controles pertinentes para mantener la SI. 10. Mejorar la eficacia y eficiencia del SGSI donde sea necesario. 11. Determinar y satisfacer las competencias necesarias para el personal que realiza tareas en la aplicación del SGSI. 12. Asegurar que todo el personal sea consciente de la importancia de sus actividades y de cómo contribuye a la consecución de los objetivos del SGSI. 13. Evaluar la necesidad de modificar el enfoque para la gestión de riesgos, el Plan de Tratamiento de Riesgos, procedimientos y/o controles en respuesta a cambios internos o externos.
Oficial de la SI (**CISO -** *Chief Information Security Officer*)	Responsable máximo de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mantener y mejorar la SI en sus dimensiones primarias: confidencialidad, integridad y disponibilidad.	1. Elaborar las políticas, normas y procedimientos de SI y gestionar su aprobación. 2. Implementar y velar por el cumplimento de las políticas, normas, y procedimientos de la SI. 3. Establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI acorde con las fases del modelo PDCA. 4. Coordinar el análisis de riesgos, planes de contingencia y prevención de desastres relacionados con el SGSI. 5. Dirigir las investigaciones sobre incidentes y problemas relacionados con la SI. 6. Planear, diseñar y ejecutar auditorías internas de la SI. 7. Recomendar las medidas pertinentes.

Líderes técnicos de las aplicaciones	Son los profesionales adscritos a la División de las TIC de la Universidad del Cauca, responsables de mantener operando las respectivas aplicaciones software y de ayudar a los usuarios finales a ser más eficaces en el desempeño de su labor.	1. Hacer el diagnóstico del inconveniente reportado por el usuario final. 2. Hacer la clasificación correspondiente al inconveniente reportado 3. Si en la clasificación la solución depende del líder técnico se procede a resolverlo. 4. Si en la clasificación de la solución depende de desarrollo, el líder técnico debe escalar la solicitud a desarrollo interno si el aplicativo es desarrollo propio o externo si la aplicación es de un proveedor externo. 5. Asumir el papel de canal de comunicación eficaz entre los usuarios finales, lideres funcionales, desarrolladores y proveedores externos
Administradores de las Bases de Datos.	Profesionales adscritos a la División de las TIC de la Universidad.	1. Garantizar accesibilidad a las diferentes bases de datos. 2. Garantizar copias de respaldo. 3. Llevar a cabo la recuperación de desastres. 4. Diseñar planes de contingencia. 5. Monitoreo del rendimiento de las Bases de datos.
Líderes funcionales de las aplicaciones	Encargados de garantizar la SI de los correspondientes activos de información institucionales. Son los respectivos Jefes de las Dependencias.	1. Definir la clasificación de la información. 2. Determinar los niveles de acceso a la información 3. Autorizar la asignación de permisos de acceso a la información 4. Apoyar a la División de las TIC en la generación de los controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información.
Administrador del SGSI en cada división institucional		1. Implementar y velar por el cumplimento de las políticas, normas, y procedimientos de SI en su División. 2. Implementar, operar, monitorear, revisar, mantener y mejorar el SGSI en su División.

		3. Apoyar las investigaciones sobre incidentes y problemas relacionados con la SI en su División. 4. Apoyar las revisiones del SGSI en su División. 5. Recomendar las medidas pertinentes.

Tabla 3.1. Roles y responsabilidades de SI

3.1.7. Actividades

A continuación se listan las actividades del presente proyecto agrupadas, según corresponda, en cada una de las 4 etapas definidas por el modelo para la construcción de soluciones propuesto por [25].

ETAPA 1: ESTUDIO DE PRE-FACTIBILIDAD

Actividad 1 Identificar los objetivos y prioridades de SI para el caso de estudio.
Actividad 2 Identificar requerimientos legales y contractuales asociados a la SI.
Actividad 3 Identificar las características de negocio.
Actividad 4 Definir el alcance preliminar del SGSI.
Actividad 5 Definir los roles y responsabilidades para la implantación del SGSI.

ETAPA 2: FORMULACIÓN DEL PROYECTO.

Actividad 6 Definir el alcance y los límites de carácter organizacional.
Actividad 7 Definir el alcance y los límites de las TIC.
Actividad 8 Definir el alcance y los límites físicos.
Actividad 9 Obtener el alcance del SGSI integrando los resultados de las actividades 5, 6 y 7.
Actividad 10 Desarrollar la política de SI.
Actividad 11 Identificar los activos cubiertos por alcance del SGSI.
Actividad 12 Identificar los requerimientos de SI.
Actividad 13 Realizar una evaluación del estado actual de la SI en el caso de estudio.

ETAPA 3: EJECUCIÓN DEL PROYECTO.

Actividad 14 Definir cuál de las técnicas ofrecidas por MAGERIT V3 para la valoración de riesgos, es la más adecuada para procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca.

Actividad 15 Definir escalas y criterios, para la valoración de activos, amenazas y salvaguardas, cuya aplicación resulte adecuada para procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca.

Actividad 16 Definir los criterios para la toma de decisiones frente a las opciones de tratamiento de riesgos.

Actividad 17 Seleccionar las tareas de MAGERIT V3 que sean aplicables a procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca.

Actividad 18 Elaborar la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3 como mecanismo para la gestión de riesgos de la SI, según los requerimientos de la norma ISO/IEC 27001 [2], en procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca.

Actividad 19 Elaborar la guía para la implementación del mecanismo de comunicación de problemas en la SI: Plantillas Genéricas de Seguridad, como una propuesta para que las dependencias de la Universidad del Cauca logren un aprendizaje colaborativo sobre los incidentes de SI.

ETAPA 4: VALIDACIÓN DE LA SOLUCIÓN.

Actividad 20 Realizar, con base en la adaptación de la metodología MAGERIT V3, la valoración de riesgos de la SI en el caso de estudio.

Actividad 21 Realizar, con base en la adaptación de la metodología MAGERIT V3, la planeación del tratamiento de riesgos de la SI para el caso de estudio.

Actividad 22 Identificar fallas en la adaptación de la metodología MAGERIT y corregir la correspondiente guía.

3.1.8. Cronograma de actividades.

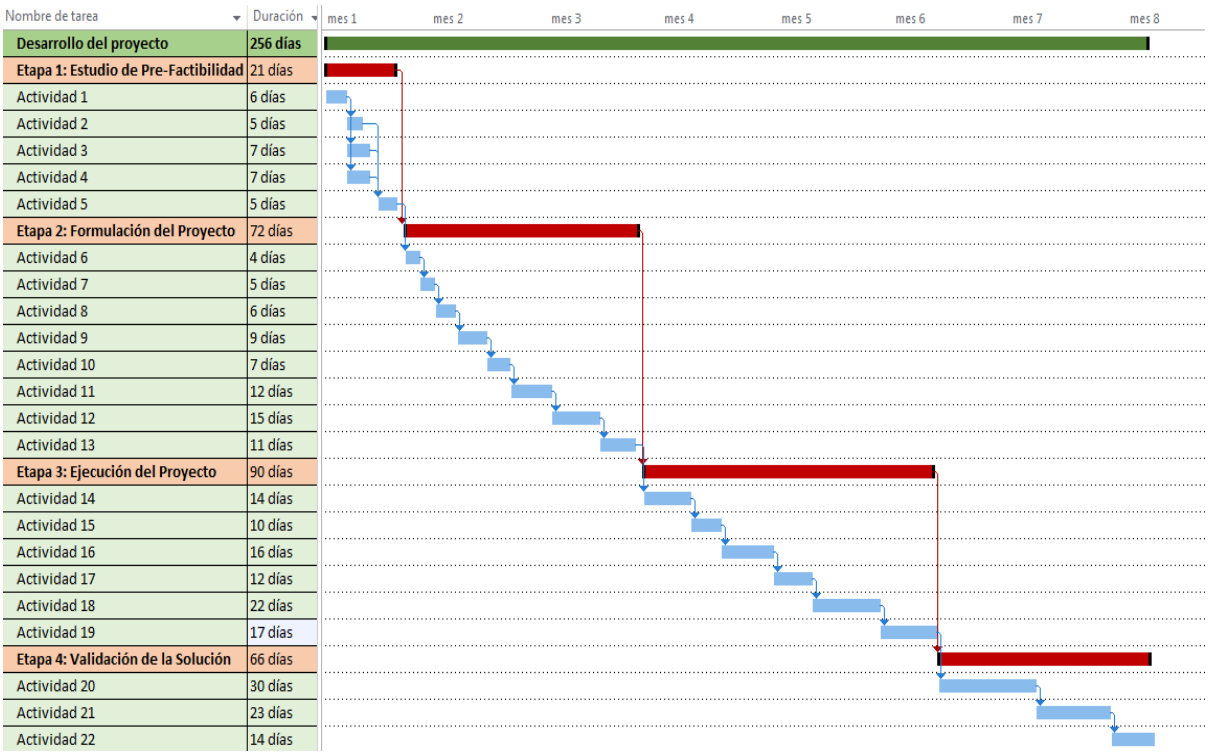

Figura 3.8. Cronograma de actividades. Fuente: propia de los autores

3.1.9. Recursos, presupuestos y fuentes de financiación.

En la Tabla 3.2 se muestra la estimación del presupuesto y de los recursos que serán necesarios para el desarrollo del presente proyecto teniendo en cuenta la tabla de criterios establecida por el Comité de Investigación de la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca, con un valor por punto de 11.246 pesos (COP) para el año 2015.

RUBROS	FUENTES		TOTAL
	ESTUDIANTES	DEPARTAMENTO	
Personal	$ 32.879.700,00	$ 1.934.100,00	$34.813.800,00
Equipo	$ 795.046,15	$ 0	$ 795.046,15
Software	$ 4.183.015,20	$ 0	$ 4.183.015,20
Bibliografía	$ 200.000,00	$ 0	$ 200.000,00
Materiales	$250.000,00	$ 0	$ 250.000,00
Comunicación	$150.000,00	$ 0	$150.000,00
Otros	$200.000,00	$ 0	$200.000,00
TOTAL	**$38.657.761,35**	**$ 1.934.100,00**	**$40.591.861,35**

Tabla 3.2. Presupuesto del proyecto

3.2. Aprobación del proyecto

Para la aprobación del proyecto se presentan dos contextos diferentes, el contexto académico y el contexto administrativo, los cuales se detallan a continuación:

3.2.1. Aprobación del proyecto en el contexto académico

La viabilidad del proyecto es determinado en el ámbito académico gracias a la evaluación de la propuesta mencionada anteriormente por parte del Consejo de Facultad de la FIET, y la determinación de la continuidad del presente proyecto, autorizando el inicio de las actividades correspondientes.

Esta decisión fue plasmada en la Resolución 8.4.2-90.14/417 de 2015, emitida el 25 de septiembre del año 2015 por el Consejo de Facultad de la FIET y mediante la cual se resuelve aprobar el anteproyecto asociado al presente trabajo. Dicha resolución es ilustrada, a continuación, por la Figura 3.9, logrando satisfacer el entregable: *"Aprobación del proyecto",* requerido por la fase 1 del proceso de planeación de un SGSI.

3.2.2. Aprobación del proyecto en el contexto administrativo

El proyecto para la implantación del Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca formalmente no ha sido aprobado por parte del Consejo Superior, el cual es el mayor órgano decisorio en la institución, sin embargo, se aprobó la Política del SGSI mediante la resolución rectoral R-785 de 2015, certificando así, en primera instancia, la viabilidad y factibilidad del proyecto de implantación del SGSI para la Universidad.

Cabe resaltar que el presente proyecto tiene como una de sus finalidades el de dar soporte al proyecto en el cual se encuentra enmarcado, el cual es la Implantación del Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca, por tal motivo, la factibilidad del presente proyecto está determinada a la factibilidad y viabilidad que está en proceso de tramitación y aprobación, la cual es gestionada por el Magister Francisco Javier Terán, Jefe de la División de TIC's de la Institución y por el Ingeniero Especialista Siler Amador Donado. A esto se añade la aprobación de este proyecto, realizada por el Jefe de la División de Gestión de la Investigación, es él quien tiene a cargo la correcta ejecución del caso de estudio y procedimiento crítico dentro de la Universidad.

Capitulo 4

Formulación del proyecto

Durante esta segunda etapa de desarrollo del proyecto se pretende analizar los aspectos esenciales relacionados con la construcción de la solución y el aseguramiento de su viabilidad. Según el estándar ISO/IEC 27003 [4], los factores claves para el desarrollo exitoso del proyecto son:

- La definición del alcance del SGSI y de las políticas de SI. Corresponden a la fase 2 del proceso de planeación de un SGSI ilustrado por la Figura 2.2. Estos aspectos son abordados, respectivamente, por las secciones 4.1 y 4.2.

- El análisis de requerimientos de SI. Corresponde a la fase 3 del proceso de planeación de un SGSI ilustrado por la Figura 2.2. Útil para identificar los activos cubiertos por el alcance y obtener una idea general del estado actual de la SI en el caso de estudio. Los resultados son expuestos por la sección 4.3.

De esta manera, la presente etapa logra abordar las fases 2 y 3 del proceso de planeación de un SGSI expuesto por la Figura 2.2, satisfaciendo, de igual manera, los respectivos entregables.

4.1. Definición del alcance del SGSI

4.1.1. Alcance organizacional

Como se mencionó en la sección 2.2.2, la metodología de las elipses puede contribuir a la determinación del alcance organizacional del SGSI aportando una clara identificación de los componentes trascendentales de la VRI, tal y como lo ilustra, a continuación, la Figura 4.1.

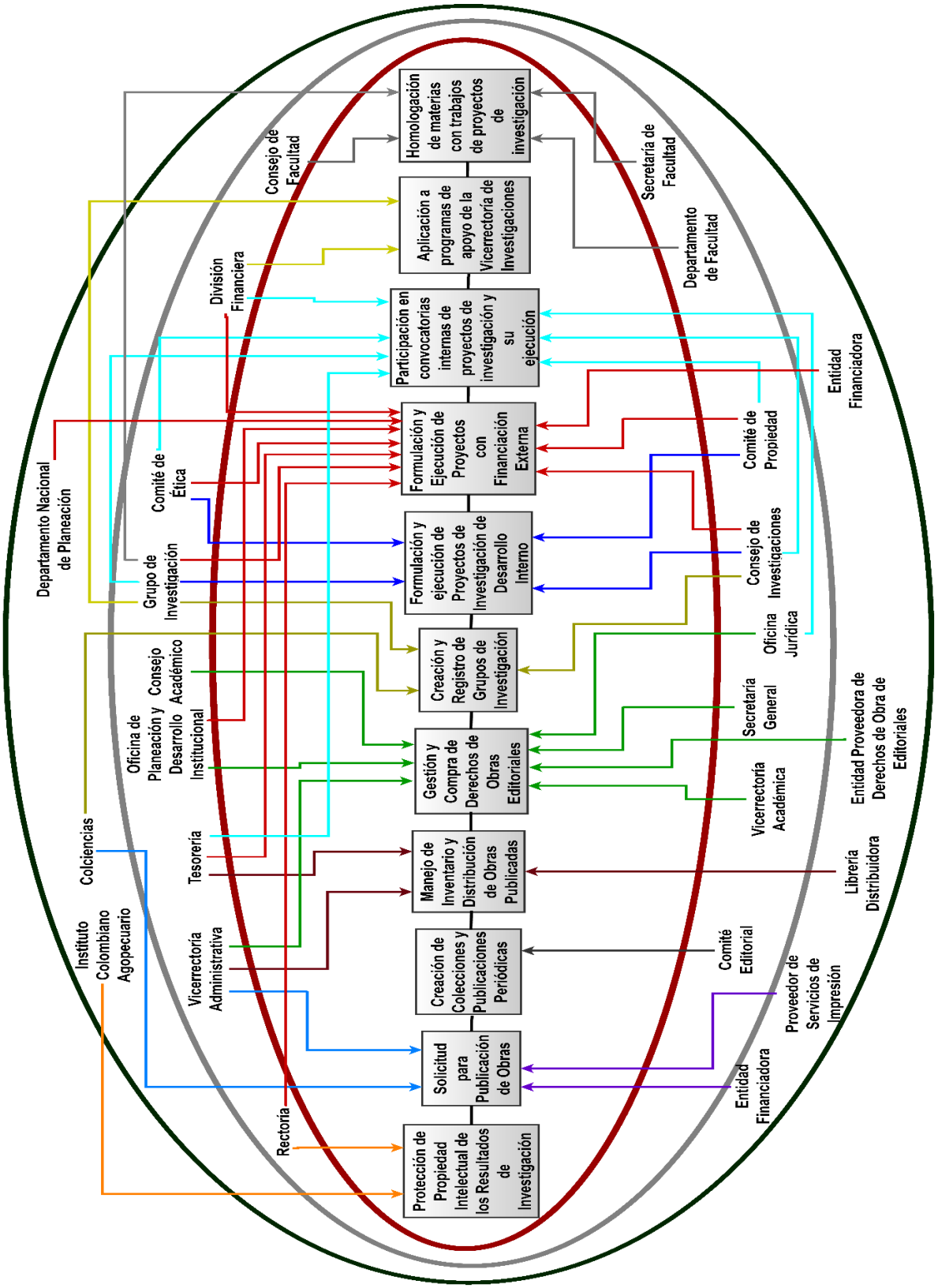

Figura 4.1. Procedimientos ejecutados por la VRI. Fuente: propia

En la Figura 4.1 se muestra una elipse interna que agrupa los procedimientos más relevantes que se ejecutan al interior de la VRI. De igual manera, se traza una elipse intermedia que acoge todos los órganos directivos, dependencias y demás entes adscritos a la Universidad del Cauca, pero que no hacen parte de la VRI, y que se relacionan de alguna u otra manera con los procedimientos identificados anteriormente. Finalmente, se define una elipse externa para agrupar todas las entidades, ajenas a la Universidad del Cauca, que se relacionan con los componentes de la VRI.

De esta manera, la Figura 4.1 evidencia que el procedimiento: *Formulación y ejecución de proyectos con financiación externa*, caso de estudio, es el componente más activo de la VRI, presentando el mayor número de interacciones, entre las cuales se resalta su relación con entes externos a la Universidad del Cauca como el Departamento Nacional de Planeación, con el que interactúa a través del aplicativo GESPROY[33] del Sistema General de Regalías.

En razón de lo expuesto, el SGSI deberá concentrarse exclusivamente en el caso de estudio, por lo cual, el alcance organizacional incluirá:

- Las unidades organizacionales adscritas a la VRI y sus respectivos servicios que, de alguna u otra manera, se vean involucradas en la ejecución del caso de estudio.
- Todo el personal vinculado a la ejecución del caso de estudio.
- La implementación de controles, solamente en el caso de estudio, para proteger las interacciones e intercambios de información con entes externos a la VRI.

Se excluye del alcance organizacional la gestión de la SI para:

- Las unidades organizacionales que, estando adscritas a la VRI, no aportan ni se ven involucradas con la ejecución del caso de estudio.
- Todo personal ajeno a las actividades del caso de estudio.
- Todas las unidades organizacionales, dependencias y demás entes de la Universidad del Cauca que sean ajenos a la VRI aun cuando participen en la ejecución del caso de estudio.
- Todas las unidades organizacionales y entidades externas a la Universidad del Cauca aun cuando participen en la ejecución del caso de estudio.

De esta manera se logra satisfacer el entregable: *Alcance organizacional y sus límites,* requerido por la fase 2 del proceso de planeación de un SGSI ilustrado por la Figura 2.2.

[33] Sistema de Gestión y Monitoreo a la Ejecución de Proyectos GESPROY- SGR

4.1.2. Alcance físico.

Todas las actividades relacionadas con el caso de estudio se ejecutan al interior del edificio de la VRI de la Universidad del Cauca, ubicado en la carrera 2 # 1A - 25 de la ciudad de Popayán, departamento del Cauca, como lo ilustra, a continuación, la Figura 4.2.

Figura 4.2. Ubicación geográfica del caso de estudio. Tomada de Google Maps

El alcance físico incluirá, exclusivamente, la gestión de la SI en:

- Las oficinas que estén asignadas a las unidades organizacionales de la VRI que desempeñen labores relacionadas con la ejecución del caso de estudio.
- Los cuartos, bodegas y áreas del edificio de la VRI donde se lleven a cabo tareas de creación, recolección, almacenamiento, procesamiento o eliminación de información pertinente a la ejecución del caso de estudio.

Se excluye del alcance físico la gestión de la SI en:

- Todas las oficinas, bodegas y áreas que, estando al interior del edificio de la VRI, no alberguen personas o actividades relacionadas con la ejecución del caso de estudio.
- Todas las instalaciones físicas, oficinas, bodegas y áreas ubicadas fuera del edificio de la VRI de la Universidad del Cauca.

De esta manera se logra satisfacer el entregable: *Alcance físico y sus límites,* requerido por la fase 2 del proceso de planeación de un SGSI ilustrado por la Figura 2.2.

4.1.3. Alcance de las TIC.

Los activos de las TIC juegan un papel protagónico e indispensable en la ejecución del caso de estudio, brindando soporte a través de soluciones informáticas como el sistema de información SIVRI y las redes de comunicaciones que le permiten interactuar con otras dependencias de la Universidad del Cauca, entidades externas y sistemas remotos como Finanzas Plus[34], SRF[35] y GESPROY.

En virtud de lo señalado, el alcance de las TIC incluirá la gestión de la SI, exclusivamente, para:

- El sistema de información SIVRI
- Los activos que soportan a SIVRI, tales como: servidores, redes de comunicaciones, computadores personales, dispositivos periféricos para el almacenamiento de información digital e impresoras.
- Los equipos auxiliares que proveen las condiciones ideales para el funcionamiento de los activos de las TIC. Por ejemplo los sistemas de alimentación ininterrumpida (UPS) y los equipos de climatización, etc.

Adicionalmente, se deberá garantizar que el caso de estudio implemente los controles necesarios para gestionar la SI durante las interacciones con activos TIC ajenos a la VRI como los sistemas de información Finanzas Plus, SRF y GESPROY.

Se excluye del alcance de las TIC la gestión de la SI para:

- Todo sistema de información ajeno a la VRI, como es el caso de Finanzas Plus, SRF y GESPROY.
- Computadores, servidores, redes de comunicaciones y cualquier activo de las TIC ajeno a la VRI.
- Todo activo de las TIC que no intervenga, participe o aporte en las actividades del caso de estudio

De esta manera se logra satisfacer el entregable: *Alcance de las TICs y sus límites,* requerido por la fase 2 del proceso de planeación de un SGSI ilustrado por la Figura 2.2.

[34] Es un sistema de información moderno, modular e integrado construido para apoyar la gestión, control y administración de los recursos financieros de organizaciones pertenecientes al sector estatal.
[35] Es una aplicación modular e integrada construida para apoyar la administración de recursos físicos de empresas estatales.

4.1.4. Alcance del SGSI

Integrado los resultados obtenidos de las secciones 4.1.1, 4.1.2 Y 4.1.3, se obtiene que el alcance del SGSI que, centrándose únicamente en el caso de estudio y sus activos, ha de incluir la gestión de la SI para:

- Las unidades organizacionales adscritas a la VRI y sus respectivos servicios que, de alguna u otra manera, se vean involucradas en la ejecución del caso de estudio.
- Todo el personal vinculado a la ejecución del caso de estudio.
- La implementación de controles, solamente en el caso de estudio, para proteger las interacciones e intercambios de información con entes externos a la VRI.
- Las oficinas que estén asignadas a las unidades organizacionales de la VRI que desempeñen labores relacionadas con la ejecución del caso de estudio.
- Los cuartos, bodegas y áreas del edificio de la VRI donde se lleven a cabo tareas de creación, recolección, almacenamiento, procesamiento o eliminación de información pertinente a la ejecución del caso de estudio.
- El sistema de información SIVRI
- Los activos que soportan a SIVRI, tales como: servidores, redes de comunicaciones, computadores personales, dispositivos periféricos para el almacenamiento de información digital e impresoras.
- Los equipos auxiliares que proveen las condiciones ideales para el funcionamiento de los activos de las TIC. Por ejemplo los sistemas de alimentación ininterrumpida (UPS) y los equipos de climatización, etc.
- La implementación de controles, solamente en el caso de estudio, para proteger las interacciones e intercambios de información con activos TIC ajenos a la VRI como los sistemas de información Finanzas Plus, SRF y GESPROY.

Se excluye del alcance del SGSI, cualquier actividad de gestión de la SI para:

- Las unidades organizacionales que, estando adscritas a la VRI, no aportan ni se ven involucradas con la ejecución del caso de estudio.
- Todo personal ajeno a las actividades del caso de estudio.
- Todas las unidades organizacionales, dependencias y demás entes de la Universidad del Cauca que sean ajenos a la VRI aun cuando participen en la ejecución del caso de estudio.
- Todas las unidades organizacionales y entidades externas a la Universidad del Cauca aun cuando participen en la ejecución del caso de estudio.
- Todas las oficinas, bodegas y áreas que, estando al interior del edificio de la VRI, no alberguen personas o actividades relacionadas con la ejecución del caso de estudio.
- Todas las instalaciones físicas, oficinas, bodegas y áreas ubicadas fuera del edificio de la VRI de la Universidad del Cauca.

- Todo sistema de información ajeno a la VRI, como es el caso de Finanzas Plus, SRF y GESPROY.
- Computadores, servidores, redes de comunicaciones y cualquier activo de las TIC ajeno a la VRI.
- Todo activo de las TIC que no intervenga, participe o aporte en las actividades del caso de estudio

De esta manera se logra satisfacer el entregable: *Alcance y límites del SGSI,* requerido por la fase 2 del proceso de planeación de un SGSI ilustrado por la Figura 2.2.

4.2. Definición de las políticas de la SI

4.2.1. Objetivos

La VRI, para el cumplimiento de su misión, visión y plan estratégico, decide gestionar la SI en el caso de estudio con el fin de:

a. Proteger los activos de información involucrados en la ejecución del caso de estudio.
b. Mitigar los riesgos de la SI que atentan contra los activos de información involucrados en la ejecución de las actividades del caso de estudio.
c. Mantener la confianza que la comunidad investigadora y las entidades externas que financian los proyectos de investigación, tienen hacia el caso de estudio, otorgándoles la garantía de que los activos de información están protegidos adecuadamente.
d. Garantizar el cumplimiento de las obligaciones contractuales con las entidades externas que financian los proyectos de investigación y evitar consecuencias legales y económicas que puedan derivarse del incumplimiento.
e. Obtener conformidad legal con los requerimientos emanados por la normativa colombiana en materia de la SI.
f. Contribuir a la implementación y certificación del SGSI de la Universidad del Cauca.
g. Brindar soporte al SGSI de la Universidad del Cauca.
h. Contribuir a la consecución de los objetivos propuestos por la política del SGSI de la Universidad del Cauca [34].
i. Apoyar la innovación tecnológica.
j. Fortalecer la cultura de SI en los estamentos universitarios, contratistas, proveedores y terceros vinculados al caso de estudio.
k. Garantizar la continuidad de las operaciones del caso de estudio frente a los incidentes de la SI.

4.2.2. Alcance de las políticas de la SI

Las políticas de SI, que aquí se establezcan, aplicarán a todos los estamentos universitarios, contratistas, proveedores, ciudadanía en general y demás terceros que se encuentren vinculados al caso de estudio y la ejecución de sus actividades.

4.2.3. Nivel de cumplimiento

Las políticas de SI, que aquí se establezcan, deberán ser cumplidas en un 100% por todos los estamentos universitarios, contratistas, proveedores, ciudadanía en general y demás terceros que sean cubiertos por el alcance de las mismas.

4.2.4. Políticas de la SI para el caso de estudio

Para demostrar su liderazgo y compromiso con la gestión de la SI, la VRI establece las siguientes políticas de la SI para el caso de estudio:

a. Política de tratamiento y protección de datos personales.
b. Política sobre el uso de la criptografía.
c. Política de control de acceso.
d. Política para la clasificación de la información.
e. Política de seguridad física.
f. Política de copias de respaldo.
g. Política de transferencia de información.
h. Política de protección contra malware.
i. Política de gestión de vulnerabilidades técnicas.
j. Política sobre la responsabilidad de los activos.
k. Política de pantalla y escritorio limpio.
l. Política de registro y auditoría.
m. Política para la seguridad en las redes de comunicaciones.
n. Política para la adquisición, desarrollo y mantenimiento de los sistemas.
o. Política para el cumplimiento de requisitos legales y contractuales.
p. Política para la continuidad de la SI

Las anteriores son expuestas, en detalle, por el Anexo D, logrando satisfacer el entregable: *Políticas de la SI,* requerido por la fase 2 del proceso de planeación de un SGSI[36].

[36] Ver la Figura 2.2.

4.3. Análisis de requerimientos de la SI

4.3.1. Identificación de los requerimientos de la SI

Como lo ilustra la Tabla 4.1, la ejecución de las actividades del caso de estudio implica la gestión de toda la información relacionada con la formulación y ejecución administrativa, jurídica, financiera y presupuestal de los proyectos que gozan de la financiación por parte de una entidad externa, incluyendo datos sensibles sobre la propiedad intelectual, derechos de autor de productos y proyectos, contratistas, investigadores y convenios con organizaciones. Por lo general, siempre existirá una copia física para toda información, la cual será gestionada por el sistema de archivo *Satélite*. Comúnmente, la transferencia de documentos impresos se materializa acudiendo al mensajero de la VRI o mediante la entrega personal. La información digital, por su parte, es creada, almacenada, procesada, recuperada y transferida por medio de los dispositivos de almacenamiento mencionados en la Tabla 4.1, el correo electrónico institucional, entre otros.

Para soportar esta información, el caso de estudio, como lo muestra la Tabla 4.1, acude al uso de activos como computadores, soportes de información, la infraestructura de red, el sistema de archivo Satélite, las instalaciones físicas, los equipos auxiliares, el Sistema de Información de la VRI (SIVRI)[37] y el indispensable personal, cuyo nivel de conciencia y conocimiento en cuestiones de la SI no va más allá de la implementación de controles sencillos como la instalación de antivirus, el uso contraseñas para el inicio de sesión en las estaciones de trabajo y el uso de archivadores para almacenar los documentos bajo llave.

Con base en estas particularidades expuestas por del caso de estudio, se identificaron los siguientes requerimientos para el SGSI:

- Definir una política para la clasificación de la información que establezca los procedimientos y controles necesarios para proteger la información de acuerdo a su importancia o relevancia para el caso de estudio, considerando los tres tipos de información definidos por el artículo 6 de la ley 1712 de 2014.
- Definir e implementar las políticas, procedimientos y controles requeridos para proteger los activos que soportan la información gestionada por el caso de estudio, incluyendo al personal y a los equipos asociados a SIVRI.
- Definir e implementar un programa de educación y entrenamiento para garantizar que el personal se encuentre totalmente capacitado y sea consciente de sus responsabilidades frente a la SI.
- Definir e implementar controles que garanticen el cumplimiento de las obligaciones legales y contractuales del caso de estudio.

[37] En SIVRI se registra la información de todos los proyectos de investigación aprobados

- Diseñar las Plantillas Genéricas de Seguridad como un mecanismo que le permita al caso de estudio comunicar los incidentes a los diferentes roles de SI de la Universidad del Cauca que fueron identificados por la Tabla 3.1. En el Anexo B se propone una guía para la implantar las Plantillas Genéricas de Seguridad.

De esta manera se logra satisfacer el entregable *"Requerimientos de SI"* correspondiente a la fase 3 del proceso de planeación de un SGSI, ilustrado por la Figura 2.2.

4.3.2. Activos de información cubiertos por el alcance del SGSI

En el capítulo 2 de la guía [23], se declara que los activos se pueden clasificar en: información, claves criptográficas, servicios, software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones y personal. Respecto a lo anterior, la norma ISO/IEC 27001 [2], sugiere que la información, a su vez, se clasifique en función de su valor y criticidad con el fin de garantizar que ésta reciba un nivel apropiado de protección de acuerdo con su importancia para la organización[38].

Particularmente en Colombia, el artículo 2 de la ley 1712 de 2014[39] [41] establece que toda información en posesión, bajo control o custodia de un *sujeto obligado* es considerada como pública y será amparada y regida por lo estipulado en dicha ley, cuyo artículo 5, establece que el término *sujeto obligado* se refiere a: las entidades públicas, personas naturales y jurídicas que presten función pública y demás entes que administren instituciones parafiscales, fondos o recursos de naturaleza u origen público.

Consecuentemente, la Universidad del Cauca y todas sus dependencias adquieren la calidad de sujetos obligados y, por ende, la información gestionada por el caso de estudio deberá ser clasificada de acuerdo a lo estipulado por el artículo 6 de la misma ley, el cual establece que la información puede tomar tres formas como lo ilustra, a continuación, la Figura 4.3.

[38] Ver el control A.8.2 que sugiere la norma ISO/IEC 27001 [2] en su Anexo A.
[39] Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

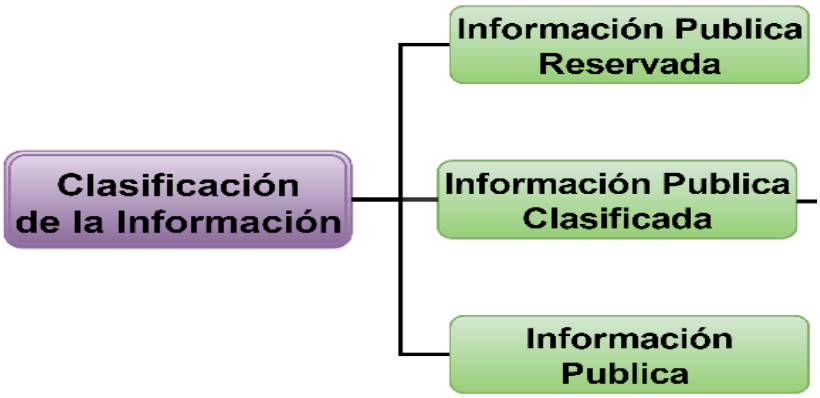

Figura 4.3. Clasificación de la información según [41]

Gracias a este hallazgo, en la sección 5.2, se propone una nueva adaptación que reemplaza los tipos de información que define MAGERIT V3 en [23], por las categorías definidas por el artículo 6 de la ley 1712 de 2014. De igual manera, en la sección 5.2 se describe detalladamente las 3 clases de información definidas por este esquema de clasificación que fue identificado gracias al documento **elaborado por la Presidencia de la República de Colombia** [42].

Clasificando la información con base en esta adaptación que se desarrolla en la sección 5.2 y agrupando los demás activos, que no sean información, como lo indica la metodología MAGERIT V3 en [23], se obtiene el inventario representado, a continuación, por la Tabla 4.1.

Nombre del activo	Descripción	Tipo
Presupuesto global de cada proyecto de investigación	Debe existir uno por cada proyecto de investigación. Describe detalladamente el presupuesto global (Personal, equipos, software, transferencias, materiales, servicios técnicos, capacitaciones, salidas, comunicaciones y transporte, etc.)	Información pública clasificada
Hojas de vida de los investigadores.	Se conserva una hoja de vida por cada investigador de cada grupo de investigación. Incluye información personal, de carácter público.	Información pública
Resumen de proyectos	Es un documento que contiene información general de los proyectos de investigación. Debe existir uno por cada proyecto	Información pública

Avales concedidos a cada proyecto de investigación.	Aval Institucional: otorgado a cada proyecto de investigación para autorizar su presentación ante la correspondiente convocatoria externa. Aval Ético: otorgado a cada proyecto de investigación para certificar sus componentes ético-legales. Aval de Propiedad Intelectual: otorgado a cada proyecto de investigación para certificar aspectos relacionados con la propiedad intelectual.	Información pública reservada
Actas de reunión del Consejo de Investigaciones y del Comité de Ética.	Registra los temas tratados y los acuerdos adoptados en cada reunión del Consejo de Investigaciones y del Comité de Ética, con la finalidad de certificar lo acontecido y dar validez a lo acordado.	Información pública clasificada
Registro de préstamo de carpetas de información	Permite asignar la responsabilidad y la custodia de las carpetas de información. Consta de una existencia que es controlada por la secretaria de la VRI.	Información pública
Pre-evaluación de proyectos	Es un documento que refleja la evaluación diligenciada por los departamentos para determinar la viabilidad de los proyectos de investigación. Debe existir uno por cada proyecto.	Información pública
Convenios - Contratos con entidades financiadoras	Documento en el cual la entidad externa se compromete a financiar el proyecto de investigación y la Universidad del Cauca a cumplir los objetivos de dicho proyecto. Debe existir uno por cada proyecto en ejecución.	Información pública reservada
Documentos de viabilidad financiera de los proyectos de investigación.	Es un documento que refleja la viabilidad financiera de cada proyecto. Mientras no exista, el contrato/convenio con la entidad externa financiadora no será firmado por el rector de la Universidad.	Información pública reservada
Oficios remisorios a las entidades externas financiadoras.	Hace referencia a todo documento u oficio que se envíe a las entidades externas que financian los proyectos de investigación. Existirán tantos como san necesarios.	Información pública clasificada

Ficha de evaluación de la Propiedad Intelectual	Plantillas para la evaluación de los componentes de los proyectos relacionados con la gestión de la propiedad intelectual	Información pública
Oficios remisorios a la División de Gestión Financiera.	Hace referencia a todo documento u oficio que se envíe a la División de Gestión Financiera. Existirán tantos como san necesarios.	Información pública clasificada
Informes financieros sobre la ejecución presupuestal de los proyectos de investigación.	Son documentos, debidamente soportados por la División de Gestión Financiera, que evidencian la ejecución presupuestal de cada proyecto (de conformidad con los plazos acordados en el convenio con la entidad externa). Serán remitidos a la entidad externa financiadora cuando sea el caso de conformidad con los requisitos y compromisos adquiridos a través del convenio, contrato u acuerdo	Información pública reservada
Informes técnicos, parciales o finales, de los proyectos de investigación.	Son documentos que evidencian el desarrollo del proyecto y los resultados obtenidos, con el fin de comprobar el cumplimiento de los compromisos adquiridos. Serán remitidos a la entidad externa financiadora cuando sea el caso de conformidad con los requisitos y compromisos adquiridos a través del convenio, contrato u acuerdo.	Información pública clasificada
Actas de Liquidación de convenios-contratos con entidades externas.	Documento donde se refleja la liquidación del contrato constituyendo su balance final o ajuste de cuentas, entre la entidad externa y la Universidad del Cauca, con miras a finiquitar, de una vez por todas, la relación jurídica obligacional.	Información pública
Certificados de Disponibilidad Presupuestal (CDP)	Es un documento mediante el cual se garantiza el principio de legalidad, es decir, la existencia del rubro y la apropiación presupuestal suficiente para atender un gasto determinado. Todos los actos administrativos, contratos y convenios deberán contar previamente con los CDP. Cualquier compromiso que se adquiera con violación de esa obligación, generará responsabilidad disciplinaria, fiscal y penal. Por cada proyecto, pueden existir tantos CDP como sean necesarios.	Información pública reservada

Ordenes de Prestación de Servicios (OPS)	Contrato en el que un individuo se obliga a prestar el servicio personal o profesional requerido para desempeñar unas actividades específicas. Por cada proyecto, pueden existir tantas OPS como sean necesarias.	Información pública reservada
Solicitud de avance para compras o comisión de servicios	Documento mediante el cual se solicita adelantos en dinero entregados a investigadores, funcionarios, docentes, estudiantes, entre otros. Por cada proyecto, pueden existir tantas solicitudes como sean necesarias.	Información pública reservada
Orden de suministros	Documento que se utiliza para solicitar a un proveedor que surta la cantidad de bienes, arrendamientos o servicios requeridos, tratándose de contratos abiertos. Por cada proyecto, pueden existir tantas órdenes como sean necesarias	Información pública reservada
Registros de Disponibilidad Presupuestal	Es un documento que refleja el perfeccionamiento del compromiso, garantizando que los recursos comprometidos no sean desviados a ningún otro fin. De acuerdo con el Art. 38 del Estatuto Presupuestal: “Los compromisos efectivamente adquiridos con cargo a las disponibilidades presupuestales expedidas deben contar también con registro presupuestal, en virtud del cual los recursos no podrán ser desviados a ningún otro fin…”. Los ordenadores de gasto y los pagadores responderán personal y pecuniariamente por incumplir lo establecido en los artículos 38 y 39 del Estatuto Presupuestal.	Información pública reservada
Órdenes de Pago	Documentos que reflejan el mandato expreso que una persona natural o jurídica (ordenante), hace a su entidad bancaria (banco emisor), para que ponga a disposición de un tercero, (beneficiario), una determinada cantidad dinero. Por cada proyecto, pueden existir tantas órdenes como sean necesarias	Información pública reservada
Planilla para entrega de correspondencia	Documento usado por la secretaría de la VRI como evidencia de la entrega de la correspondencia a sus respectivos destinatarios.	Información pública

Servicio de secretaría de la VRI	Servicio responsable de: recepcionar, registrar y distribuir la correspondencia de la VRI, emitir correspondencia bajo numeración consecutiva, atención diaria de la agenda del vicerrector de Investigaciones, cumplir y hacer cumplir las políticas, normas y procedimientos de la VRI, gestión del sistema de archivo Satélite y radicación y remisión de la documentación relacionada con los proyectos de investigación.	Servicios
Servicio de Apoyo al Investigador	Servicio que ofrece asesoría a los grupos de investigación en lo concerniente a, convocatorias, manejo administrativo de los proyectos formulados, estrategias de financiamiento y documentación relacionada con la ejecución de los proyectos de investigación.	Servicios
SIVRI (Sistema de Información de la VRI)	Conjunto de componentes que recolectan, generan, almacenan y procesan la información gestionada por la VRI.	Software
Documentos físicos	Testimonio material de un hecho o acto realizado por funcionarios de la VRI en el ejercicio de sus funciones en cualquier tipo de soporte (papel, cintas, discos magnéticos, fotografías, etc.)	Soporte de información
Dispositivos de almacenamiento de información digital.	Algunos ejemplos de estos dispositivos son los discos duros, memorias USB, CDs, DVDs, entre otros	Soporte de información
Servidores	Equipos informáticos cuyo propósito es soportar el SIVRI. Actualmente existen tres y se encuentran dotados de los sistemas operativos Microsoft Windows Server 2008 y 2012. Ejecutan servidores de aplicaciones para desarrollos con Java Enterprise Edition 7 y proveen un gestor de bases de datos ORACLE versión 11g. Se encuentran ubicados en el cuarto de servidores de la VRI.	Combinación de software y hardware

Computadores personales	Computadores portátiles y de escritorio que son usados por el personal en el cumplimiento de sus funciones relacionadas con el caso de estudio. Siete de ellos están equipados con los sistemas operativos Windows 7/8/10 y uno con Macintosh OS X 10.10, cada uno de los cuales se encuentra ubicado en las correspondientes oficinas del personal.	Combinación de software y hardware
Fotocopiadora multifuncional	Periférico que ofrece las funciones de impresora, escáner y fotocopiadora. En la ejecución del caso de estudio intervienen tres dispositivos de esta naturaleza, uno de ellos ubicado en la secretaría de la VRI y los restantes en las oficinas del personal.	Hardware
Redes de área local	Para la ejecución de las actividades del caso de estudio, el personal hace uso tanto de la red cableada LAN como de la red inalámbrica WLAN. Cada una está asociada a un distinto segmento de la red interna de la Universidad del Cauca.	Redes de comunicación
Satélite	Toda la información involucrada por el caso de estudio deberá tener una copia física que será gestionada por Satélite; el sistema de archivo de la VRI Para su funcionamiento se dispone de varios archivadores que se encuentran ubicados al frente de la oficina de la secretaría, en el segundo piso del edificio de la VRI.	Equipamiento auxiliar
Reloj radicador	Este dispositivo es utilizado por la secretaria de la VRI para radicar la correspondencia y la documentación recibida.	Equipamiento auxiliar
Equipos de Climatización	Equipos destinados a mantener las condiciones térmicas ideales para el correcto funcionamiento de los servidores que soportan el SIVRI.	Equipamiento auxiliar
UPS	Dispositivos que, gracias a sus baterías, pueden proporcionar energía eléctrica durante un apagón. Actualmente, cinco dispositivos de esta naturaleza soportan los equipos informáticos asociados al caso de estudio.	Equipamiento auxiliar

Personal vinculado al caso de estudio.	Todos los funcionarios y contratistas de la VRI que desempeñan labores asociadas con el caso de estudio, incluyendo: el vicerrector de investigaciones, el Jefe de la División: Gestión de la Investigación, la secretaria de la VRI, el técnico administrativo de apoyo al investigador y demás contratistas. Para un total de 8 personas.	Personal
Oficinas del personal	Recintos asignados a los funcionarios y contratistas para el desarrollo de sus labores asociadas al caso de estudio. Actualmente se disponen de 6 oficinas; cinco de ellas ubicadas en el segundo piso del edificio de la VRI, mientras que la restante se ubica en el tercer piso.	Instalaciones
Cuarto de servidores	Recinto dotado con las condiciones adecuadas para alojar los servidores que dan soporte al SIVRI. Se encuentra ubicado contiguo a la oficina 209 del segundo piso del edificio de la VRI	Instalaciones
Almacén Archivo Satélite VRI	Recinto adecuado para almacenar toda la información gestionada por la VRI y que se encuentra en formato físico. Se encuentra ubicado frente a la oficina de la secretaría.	Instalaciones

Tabla 4.1. Activos cubiertos por el alcance. Fuente: propia de los autores

Cabe mencionar que fue el jefe de la División de Gestión de la Investigación, responsable del caso de estudio y propietario de la información que éste procedimiento gestiona, quien llevo a cabo la clasificación de la misma con base en el esquema discutido anteriormente. Al obtener el inventario de activos, representado por la Tabla 4.1, se logra satisfacer los entregables "*Activos identificados"* y "*Clasificación de activos",* los cuales son requeridos por la fase 3 del proceso de planeación de un SGSI ilustrado por la Figura 2.2.

4.3.3. Evaluación del estado actual de la SI.

Los requerimientos anteriormente identificados reflejan el nivel de SI deseado para el caso de estudio y sus activos de información. En contraste con lo anterior, se identificaron fuertes debilidades del caso de estudio en materia de la SI, pues actualmente:

- No se ha definido ninguna política para la clasificación de la información y, en consecuencia, tampoco se ha diseñado ni implementado control alguno que permita clasificar y proteger, de manera adecuada, la información de acuerdo a su valor e importancia, desconociendo que la mayor parte de los activos corresponden a información pública reservada[40].

- No se han diseñado ni implementado los controles necesarios para proteger los activos que soportan la información gestionada por el caso de estudio. De este modo, se evidencia una desatención generalizada por la SI y un desconocimiento total de los controles que la norma ISO/IEC 27001 sugiere en su anexo A.

- No se ha definido ningún programa de educación o entrenamiento que garantice la capacidad e idoneidad del personal en materia de la SI.

- No se contemplan controles ni medidas que persigan el cumplimiento de los requerimientos legales en materia de la SI, dejando, a la Universidad del Cauca, expuesta a las sanciones estipuladas por la normativa colombiana que fácilmente pueden ascender a los 2000 salarios mínimos e incluso, a la clausura total y definitiva de las operaciones involucradas[41].

Lo anterior representa las principales vulnerabilidades identificadas para el caso de estudio. No obstante, de estas se derivan muchas otras, como las mencionadas por el estándar ISO/IEC 27005 [5] en su Anexo D.1.

Gracias a esta evaluación del estado actual de la SI en el caso de estudio, se logra satisfacer el entregable *"Estado de la SI en la organización"* correspondiente a la fase 3 del proceso de planeación de un SGSI como lo ilustra la Figura 2.2. Cabe mencionar que, de estas actividades, solamente se está obteniendo información preliminar acerca del estado actual del caso de estudio en materia de la SI que, en conjunto con las prioridades, objetivos de SI y los requerimientos legales y contractuales identificados previamente, se usará como un incentivo para las actividades de implantación del SGSI. La fase 4 del proceso de planeación de un SGSI[42] será la encargada de entregar información más detallada, precisa y realista.

[40] Como lo evidencia la Tabla 4.1. Activos cubiertos por el alcance.
[41] Así lo estipulan el artículo 23 de la ley estatutaria1581 de 2012 [37] y el artículo 18 de la ley estatutaria 1266 de 2008 [36].
[42] Dicha fase es abordada, más adelante, en el capítulo 6

Capitulo 5

Ejecución del proyecto

Durante esta tercera etapa se pretende construir la solución del proyecto, cuyo objetivo general es adaptar la metodología MAGERIT V3 como mecanismo para la gestión de riesgos de la SI, según los requerimientos de la norma ISO/IEC 27001 [2], para el caso de estudio.

5.1. Adaptaciones necesarias

Según el estándar ISO/IEC 27005 [5], el enfoque definido para la gestión de riesgos debería ser adecuado para el entorno de la organización y parte integral de todas sus actividades asociadas con la SI, por ende, resulta de vital importancia que, antes de aplicar la metodología MAGERIT V3, ésta sea adaptada al contexto de la organización.

En razón de lo expuesto, el estándar ISO/IEC 27005 y la norma ISO/IEC 27001 establecen que, para lograr resultados de calidad, precisos, realistas, objetivos, reproducibles e independientes de la arbitrariedad del analista, el enfoque para la gestión de riesgos deberá incluir los artefactos listados por la Tabla 5.1, tal y como se muestra a continuación:

ARTEFACTO	¿LO POSEE MAGERIT V3?
Un esquema para la clasificación de la información que contemple el contexto del caso de estudio.	PARCIALMENTE
Criterios para la valoración de activos.	PARCIALMENTE
Criterios para la valoración de amenazas.	NO

Criterios para la evaluación del riesgo	**NO**
Una organización para operar la gestión de riesgos de la SI que considere la estructura funcional de la Universidad del Cauca.	**NO**
Criterios para el tratamiento del riesgo.	**NO**
Criterios para valorar las salvaguardas.	**NO**
Formalización de la aceptación de riesgos	**NO**

Tabla 5.1. Artefactos necesarios para una adecuada gestión de riesgos

Lo anterior refleja las insuficiencias de MAGERIT V3 con respecto a los artefactos demandados por la norma ISO/IEC 27001 y el estándar ISO/IEC 27005. Por ende, para adaptar MAGERIT V3 al caso de estudio, se deberá agregar 8 nuevas actividades al Método de Análisis de Riesgos (MAR) propuesto por esta metodología, con el fin de resolver cada una de sus 8 insuficiencias. Dichas actividades son presentadas a continuación:

- Definir un esquema para la clasificación de la información.
  Con esta actividad se pretende dotar al MAR con un mecanismo que permita clasificar la información tratada por el caso de estudio de acuerdo con lo estipulado por la normativa colombiana vigente y aplicable en entidades públicas como la Universidad del Cauca.

- Definir criterios para la valoración de activos.
  Con esta actividad se pretende dotar al MAR con criterios que, estando alineados con el contexto del caso de estudio, permitan valorar los activos de manera objetiva y reproducible.

- Definir criterios para la valoración de amenazas.
  Con esta actividad se pretende dotar al MAR con criterios que permitan valorar, de manera objetiva y reproducible, las amenazas que atentan contra los activos vinculados al caso de estudio.

- Definir criterios para la evaluación del riesgo.
  Con esta actividad se busca dotar al MAR con criterios que permitan evaluar el riesgo con el fin de identificar las prioridades para el tratamiento de los mismos.

- Definir criterios para la valoración de salvaguardas.
  Con esta actividad se pretende dotar al MAR con criterios que permitan valorar, de manera objetiva, las salvaguardas seleccionadas y hagan posible la estimación del riesgo residual.

- Definir criterios para el tratamiento del riesgo.
  Con esta actividad se pretende dotar al MAR con criterios que permitan seleccionar, de manera objetiva y reproducible, la opción de tratamiento más adecuada para mitigar cada riesgo identificado.

- Aceptación de riesgos.
  Por recomendación del estándar ISO/IEC 27005 [5], se agregó esta actividad, al MAR, con el propósito de formalizar la aprobación del PTR y de los riesgos residuales.

- Definir la organización para la gestión del riesgo.
  Con esta actividad se pretende definir, formalmente, una organización del personal que considere la estructura funcional de la Universidad del Cauca, definiendo los roles y responsabilidades con respecto a las actividades de gestión de riesgos de la SI.

Como producto de estas adaptaciones se obtiene el *Método de Análisis de Riesgos Adaptado* (MARA). MARA es el resultado de adaptar la metodología MAGERIT V3 como mecanismo apropiado para la gestión de riesgos de la SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca.

A continuación, la Figura 5.1 expone el MAR: el método que MAGERIT V3 originalmente propone y, en seguida, la Figura 5.2 ilustrará el MARA: el nuevo método de análisis de riesgos que se obtuvo como resultado de las adaptaciones.

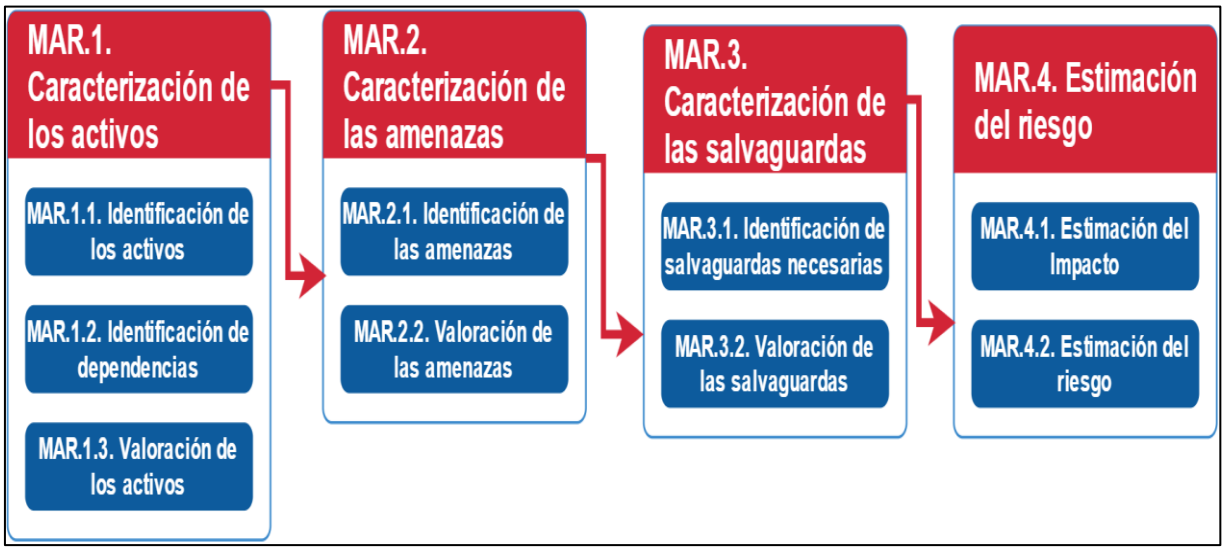

Figura 5.1. MAR: versión original de MAGERIT V3. Tomada de [22]

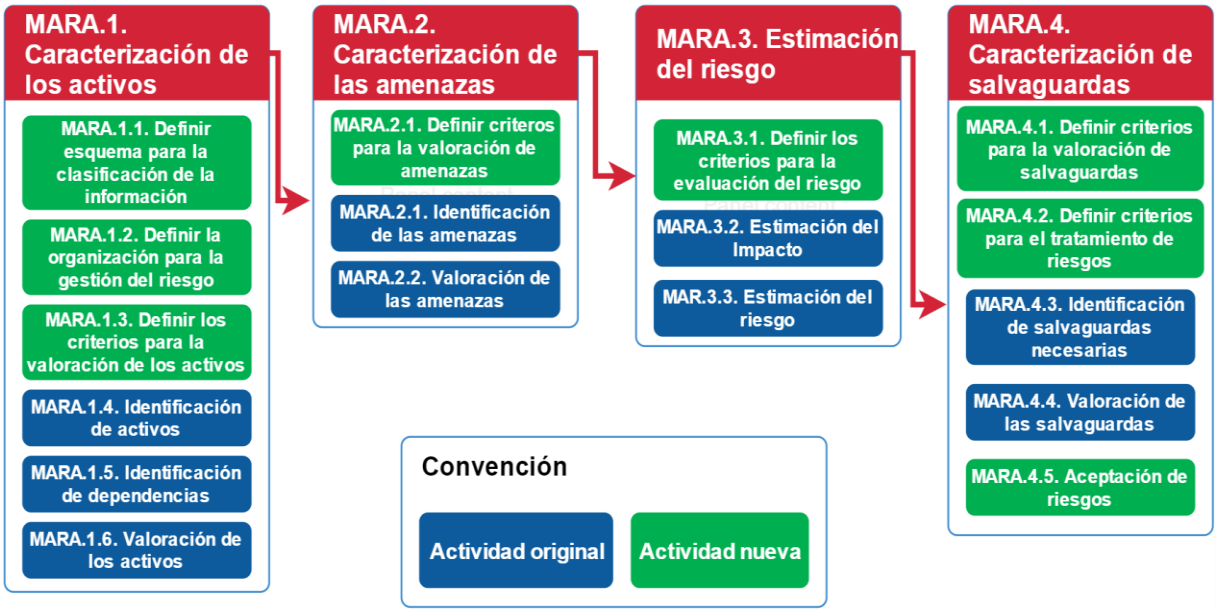

Figura 5.2. MARA: versión adaptada de MAGERIT V3. Fuente: propia

IMPORTANTE

Cabe recordar que en la sección 2.3.2 se identificó que el MAR, en su versión original, pretende seleccionar los controles necesarios para tratar el riesgo sin antes haber estimado el riesgo mismo, constituyendo un serio incumplimiento a las cláusulas 6.1.2 y 6.1.3 de la norma ISO/IEC 27001 [2], en las cuales se establece que la selección de los controles debe llevarse a cabo solamente después de:

1. Identificar y analizar los riesgos (incluye la estimación de los niveles de riesgo).
2. Evaluar los riesgos para obtener una lista de prioridades para el tratamiento.

Para evitar que se seleccionen salvaguardas sin antes haber estimado el nivel de riesgo y, así, subsanar el incumplimiento de los requerimientos emanados por la norma ISO/IEC 27001 [2], fue necesario invertir el orden de ejecución de las tareas MAR.3: *Caracterización de las salvaguardas* y MAR.4: *Estimación del estado del riesgo*, redefiniendo las respectivas entradas y salidas de acuerdo con los lineamientos ofrecidos por el estándar ISO/IEC 27005 [5].

Lo anterior evidencia cómo el MARA determina lo que se debe hacer para lograr adaptar MAGERIT V3 al caso de estudio, solamente resta definir una guía que sirva de manual al usuario, que indique cómo debe ejecutar cada tarea del MARA y que otorgue la posibilidad de que cualquier persona pueda usar la adaptación como mecanismo para gestionar los riesgos de la SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca.

En virtud de lo señalado, la sección 5.2 describe cada una de tareas formalizadas por el MARA, mientras que la sección 5.3 expone la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3 al caso de estudio.

5.2. Descripción de la adaptación propuesta

5.2.1. MARA.1. Caracterización de los activos

MARA.1. Caracterización de los activos **MARA.1.1. Definir un esquema para la clasificación de la información**
La norma ISO/IEC 27001 [2], establece que la información se debe clasificar en función de su valor y criticidad con el fin de garantizar que ésta reciba un nivel apropiado de protección de acuerdo con su importancia para la organización[43] En relación con lo anterior, la sección 4.1 del documento [23] evidencia que MAGERIT V3 reconoce dos opciones para clasificar la información: el esquema nacional de España[44] y el de la Unión Europea[45]. Sin embargo, por obvias razones, ninguno estará alineado con la normativa colombiana, por lo cual resultarán inadecuados para gestionar los riesgos de la SI en procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca. Con esta actividad se pretende obtener un esquema que permita una adecuada clasificación de la información de acuerdo con lo establecido por la normativa colombiana y demás particularidades del contexto que rodea al caso de estudio.
Objetivo: establecer un esquema para la clasificación de la información que sea adecuado para el caso de estudio.
Productos de entrada: normativa colombiana relacionada con la clasificación de la información en instituciones públicas.
Productos de salida: esquema para la clasificación de la información.
Guía:

[43] Ver el control A.8.2 que sugiere la norma ISO/IEC 27001 [2] en su Anexo A.
[44] Define 5 categorías: Secreta, Reservada, Confidencial, Difusión Limitada y Sin Clasificar.
[45] Define 4 categorías: TRES SECRET UE, SECRET UE, CONFIDENTIEL UE, RESTREINT UE.

En la sección 5.3.1 de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se suministra un esquema para la clasificación de la información. Se recomienda usar este aporte o, bien, tomarlo como punto de partida para crear un nuevo esquema que se ajuste a las necesidades y particularidades del procedimiento sobre el cual se vayan a gestionar los riesgos de SI.

Tabla 5.2. Descripción de la actividad MARA 1.1

MARA.1. Caracterización de los activos **MARA.1.2. Definir la organización para la gestión del riesgo**
Según el estándar ISO/IEC 27005 [5], el enfoque definido para la gestión de riesgos debe ser parte integral de todas las actividades de la organización en materia de la SI. Respecto a lo anterior, MAGERIT V3 solamente suministra una matriz de asignación de responsabilidades que, por ser tan genérica, no contempla la estructura organizacional de la Universidad del Cauca, por ende, no será apropiada para operar la gestión de riesgos de la SI en el caso de estudio. En razón de lo expuesto, con esta actividad se buscara definir los roles y responsabilidades del personal involucrado en la gestión de riesgos, definiendo una organización que sea adecuada y que contemple la estructura de la Universidad del Cauca.
Objetivo: Definir la organización para la gestión de riesgos de la SI.
Productos de entrada: estructura organizacional de la Universidad del Cauca
Productos de salida: una organización del personal que asigne claramente los roles y responsabilidades del personal frente a las actividades de la gestión de riesgos
Guía: Acoger las sugerencias suministradas por la sección 5.3.2 de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3.

Tabla 5.3. Descripción de la actividad MARA 1.2

MARA.1. Caracterización de los activos **MARA.1.3. Definir los criterios para la valoración de activos**
En [22], MAGERIT V3 manifiesta que la valoración no debe centrarse en el costo de adquisición o reposición de los activos, sino más bien en la importancia que estos tienen para la organización y en el nivel de protección que requieren. Respecto a lo anterior, el Centro Criptológico Nacional de España, en el marco del Esquema Nacional de Seguridad, sugiere, mediante la guía CCN-STIC-803 [50], un amplio conjunto de criterios que deberán ser adaptados al contexto normativo establecido por las leyes colombianas con el fin de adecuarlos al caso de estudio.

En razón de lo expuesto, resulta necesario establecer el conjunto de criterios, que estando alineado con el contexto del caso de estudio, permita valorar los activos en términos de su importancia para la Universidad del Cauca y de las consecuencias que se pueden desencadenar en caso de que éstos se vean comprometidos.
Objetivo: Establecer un conjunto de criterios para la valoración de activos que se ajuste al contexto del caso de estudio.
Productos de entrada: los criterios propuestos por la guía CCN-STIC-803 [50]
Productos de salida: un conjunto de criterios que, ajustados al contexto del caso de estudio, permitan valorar los activos de información en términos de su importancia y de las consecuencias que sufriría la Universidad en caso de que éstos se vean comprometidos
Guía: En el apartado 5.3.3, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se suministra una completa orientación en todo lo relacionado con la valoración de los activos. Así, en la sección 5.3.3 se propone un conjunto de criterios que ya se encuentra alineado con el contexto del caso de estudio. Se recomienda usar este aporte o, bien, tomarlo como punto de partida para ajustarlo a las necesidades y particularidades del procedimiento sobre el cual se vaya a gestionar los riesgos de SI. Finalmente, en la sección 5.3.3 se describen las instrucciones para cargar PILAR con todos los criterios que aquí se definan y lograr, de esa manera, aprovechar todos los beneficios que se pueden obtener al usar esta herramienta durante la valoración de los activos.

Tabla 5.4. Descripción de la actividad MARA 1.3

MARA.1. Caracterización de los activos **MARA.1.4. Identificación de los activos**
Con esta tarea se pretende identificar los activos vinculados al caso de estudio, determinando sus características y atributos; clasificación la información de acuerdo al esquema obtenido de la tarea MARA.1.1 y agrupando los demás activos según la tipificación suministrada por la metodología MAGERIT V3 en [23].
Objetivo: identificar los activos vinculados al caso de estudio.
Productos de entrada: los criterios propuestos por la guía CCN-STIC-803 [50]
Productos de salida: relación de activos a considerar.
❖ **Guía:** Examinar, detenidamente, el documento del procedimiento para identificar los activos vinculados al caso de estudio, clasificando la información de acuerdo con el esquema obtenido de la tarea MARA.1.1. Se recomienda que, en lo posible, se complemente esta fuente de información con entrevistas y encuestas dirigidas al personal vinculado, en especial, al jefe de división responsable del caso de estudio.

En la sección 5.3.1, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se expone una detallada guía en todo lo relacionado con la clasificación de activos.
Observaciones: Cabe mencionar que la versión original de esta tarea define varios productos de entrada que fueron excluidos de la versión adaptada porque ya estaban incluidos en el documento del procedimiento. Dichos productos son: Inventario de información, inventario de servicios prestados, procesos de negocio, diagramas de flujo de datos. De igual manera, la versión original de esta actividad definía 3 salidas: • Relación de activos a considerar • Caracterización de los activos: valor propio y acumulado • Relaciones entre activos Sin embargo, el valor de los activos, y las relaciones o dependencias entre los mismos, sólo podrán ser determinadas una vez se hayan completado las actividades MARA.1.2: *Identificación de dependencias entre activos* y MARA.1.3: *Valoración de los Activos.* Esta es la razón por la cual dichos elementos no fueron considerados como salida de esta tarea en su versión adaptada.

Tabla 5.5. Descripción de la actividad MARA 1.4

MARA.1. Caracterización de los activos **MARA.1.5. Identificación de dependencias**
Con esta actividad se pretende identificar las dependencias existentes entre los activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.
Objetivo: identificar las dependencias existentes entre los activos vinculados al caso de estudio
Productos de entrada: *el documento del procedimiento*[46] y el producto de la tarea anterior: *Relación de activos a considerar*.
Productos de salida: diagrama de dependencias entre activos.
Guía: Seguir las orientaciones que MAGERIT V3 suministra en el capítulo 3 y la sección 8.3 del documento [22].
Observaciones: Cabe mencionar que la versión original de esta tarea define varios productos de entrada que fueron excluidos de la versión adaptada porque ya estaban incluidos

[46] incluye el diagrama de flujo del procedimiento, flujo de información y el inventario de información.

en el documento del procedimiento. Dichos productos son: procesos de negocio y diagramas de flujo de datos.

Tabla 5.6. Descripción de la actividad MARA 1.5

MARA.1. Caracterización de los activos **MARA.1.6. Valoración de los activos.**
Con esta actividad se pretende valorar todas las dimensiones de los activos vinculados al caso de estudio. En [22], MAGERIT V3 manifiesta que la valoración no debe centrarse en el costo de adquisición o reposición de los activos, sino más bien en la importancia que estos tienen para la organización y en el nivel de protección que requieren.
Objetivo: valorar los activos vinculados al caso de estudio en términos de su importancia y del nivel de protección que éstos requieren.
Productos de entrada: los *criterios para la valoración de activos* definidos por la tarea MARA.1.3, y los productos de las tareas previas: "*Relación de activos a considerar"* y "*Diagrama de dependencias entre activos"*.
Productos de salida: el *Modelo de Valor* (informe del valor de los activos).
Guía: En [22] MAGERIT V3 declara que para lograr la valoración de los activos se debería entrevistar al personal vinculado en la ejecución del caso de estudio, en especial, a los directivos como el jefe de división responsable del caso de estudio. También se recomienda seguir las demás orientaciones brindadas por MAGERIT V3 suministra en el capítulo 3 del documento [22].

Tabla 5.7. Descripción de la actividad MARA 1.6

5.2.2. MARA.2. Caracterización de las amenazas

MARA.2. Caracterización de las amenazas **MARA.2.1. Definir los criterios para la valoración de amenazas.**
En [22], MAGERIT V3 declara que para poder valorar la influencia que una amenaza tiene sobre el valor de los activos, se deberá determinar su probabilidad de ocurrencia y la degradación que ésta pueda llegar causar. El estándar ISO/IEC 27005 [5] recomienda desarrollar criterios que permitan realizar estas valoraciones de manera objetiva y reproducible, sin embargo, MAGERIT V3 no dispone de ellos, pese a las sugerencias del estándar. Bajo estas condiciones, la única opción sería atar la gestión de riesgos a los datos predeterminados que ofrece la herramienta

PILAR en su catálogo de amenazas, lo cual no sería muy conveniente si consideramos que las organizaciones y sus contextos nunca serán idénticos.
Objetivo: definir los criterios para la valoración de las amenazas.
Productos de entrada: metodologías para la gestión de riesgos de la SI que, estando alineadas con el estándar ISO/IEC 27005 [5], ofrezcan cualquier material relacionado con los criterios para la valoración de las amenazas.
Productos de salida: los criterios para la valoración de las amenazas.
Guía: En el apartado 5.3.4, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se suministra una completa orientación en todo lo relacionado con la valoración de las amenazas. Así, en la sección 5.3.4 se propone adoptar unos criterios propuestos por NIST, los cuales resultaron ser completamente compatibles con la metodología MAGERIT V3 e interoperables con PILAR, permitiendo sacarle el mayor provecho a esta herramienta de apoyo. Se recomienda seguir las orientaciones suministradas por la sección 5.3.4 y, en caso de ser necesario, ajustar sus directrices a las necesidades y particularidades del procedimiento sobre el cual se vaya a gestionar los riesgos de SI.

Tabla 5.8. Descripción de la actividad MARA 2.1

MARA.2. Caracterización de las amenazas **MARA.2.2. Identificación de las amenazas**
Objetivo: identificar las amenazas que puedan atentar contra los activos vinculados al caso de estudio**.**
Productos de entrada: informe de vulnerabilidades y los productos de salida de la tarea MARA.1. *Caracterización de los activos*.
Productos de salida: Relación de amenazas posibles.
Guía: La herramienta PILAR cuenta con una biblioteca de datos estándar que provee un amplio catálogo de las amenazas más comunes[47]. Se recomienda identificar cuáles amenazas, de las listadas por dicho catálogo, atentan contra los activos vinculados al caso de estudio.

Tabla 5.9. Descripción de la actividad MARA 2.2

[47] Para acceder a dicho catálogo, inicie la aplicación PILAR y examine las amenazas contempladas por esta herramienta. Se recomienda consultar el manual de PILAR [47]

MARA.2. Caracterización de las amenazas **MARA.2.3. Valoración de las amenazas**
Objetivo: estimar la probabilidad de ocurrencia de las amenazas y la degradación que éstas pueden causar sobre el valor de los activos.
Productos de entrada: los *criterios para la valoración de amenazas*, informe de vulnerabilidades, histórico de incidentes y el producto de salida de la tarea anterior: *Relación de amenazas posibles*.
Productos de salida: el *Mapa de Riesgos* (es un informe de amenazas posibles, caracterizadas por su probabilidad de ocurrencia y la degradación que pueden llegar a causar en los activos).
Guía: La herramienta PILAR cuenta con una biblioteca de datos estándar que provee un amplio catálogo de las amenazas más comunes. Se recomienda utilizar los valores ofrecidos por PILAR como punto de partida e ir ajustándolos al contexto del caso de estudio mediante el uso de los criterios para la valoración de amenazas que se proponen en la sección 5.3.4.
Observaciones: Cabe mencionar que la versión original de esta tarea define los siguientes productos de entrada: series históricas de incidentes y antecedentes de incidentes en la organización. Para favorecer la practicidad, la versión adaptada de esta tarea unifica estas entradas en un solo producto: *Histórico de incidentes.*

Tabla 5.10. Descripción de la actividad MARA 2.3

5.2.3. MARA.3. Estimación del estado del riesgo

MARA.3. Estimación del estado del riesgo **MARA.3.1. Definir criterios para la evaluación del riesgo**
La cláusula 6.1.2 de la norma ISO/IEC 27001 [2] establece que los riesgos deben ser evaluados a fin de identificar las prioridades para el tratamiento de los mismos. Respecto a lo anterior, el estándar ISO/IEC 27005 [2] sugiere desarrollar criterios que permitan evaluar el riesgo de manera objetiva y reproducible, sin embargo, MAGERIT V3 no dispone de ellos, pese a las sugerencias del estándar. En razón de lo expuesto, resulta necesario definir criterios que, estando alineados con el contexto del caso de estudio, permitan evaluar los riesgos de manera objetiva y reproducible.
Objetivo: definir los criterios para la evaluación de los riesgos de SI.

Productos de entrada: la escala para la representación del nivel de riesgo que se propone en [47].
Productos de salida: los criterios para la evaluación de los riesgos de SI.
Guía: En el apartado A.5, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se suministra una completa orientación en todo lo relacionado con la evaluación del riesgo.

Tabla 5.11. Descripción de la actividad MARA 3.1

MARA.3. Estimación del estado del riesgo **MARA.3.2. Estimación del impacto**
Con esta tarea se pretende estimar el impacto potencial al que se encuentran expuestos los activos vinculados al caso de estudio, para lo cual se deberá tener en cuenta los controles o salvaguardas existentes.
Objetivo: determinar el impacto potencial al que se encuentran sometidos los activos de información vinculados al caso de estudio.
Productos de entrada: productos de salida de las tareas MARA.1. *Caracterización de los activos* y MARA.2. *Caracterización de las amenazas*.
Productos de salida: informe de impacto potencial.
Guía: En la sección 2.2 de la guía de técnicas [24], ofrecida por MAGERIT V3, se suministran los lineamientos necesarios para calcular el impacto potencial que causan las amenazas sobre los activos vinculados al caso de estudio. Adicionalmente se puede acudir al apoyo que ofrece MAGERIT V3 en lo relacionado con este tipo de estimaciones.

Tabla 5.12. Descripción de la actividad MARA 3.2

MARA.3. Estimación del estado del riesgo **MARA.3.3. Estimación del riesgo**
Con esta tarea se pretende estimar el riesgo potencial al que se encuentran expuestos los activos vinculados al caso de estudio, identificando claramente las prioridades de tratamiento mediante la aplicación de los criterios para la evaluación de riesgos.
Objetivo: determinar el riesgo potencial al que se encuentran sometidos los activos de información vinculados al caso de estudio e identificar las prioridades para el tratamiento de riesgos.
Productos de entrada: los criterios para la evaluación de los riesgos, el *Informe de impacto potencial* y el *Mapa de Riesgos* obtenido de la tarea MARA.2.3.
Productos de salida: informe de riesgo potencial.
Guía:

En la sección 2.2 de la guía de técnicas [24], ofrecida por MAGERIT V3, se suministran los lineamientos necesarios para calcular el nivel de riesgo al que se exponen los activos vinculados al caso de estudio. En el apartado A.5, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se suministra una completa orientación en todo lo relacionado con la evaluación del riesgo. Adicionalmente se puede acudir al apoyo que ofrece MAGERIT V3 en lo relacionado con este tipo de estimaciones.

Tabla 5.13. Descripción de la actividad MARA 3.3

5.2.4. MARA.4. Caracterización de las salvaguardas

MARA.4. Caracterización de las salvaguardas **MARA.4.1. Definir criterios para la valoración de salvaguardas**
Según el estándar ISO/IEC 27005 [5], una vez definido el PTR, se deberá estimar los riesgos residuales a los que se enfrentará la organización después de que se implementen los controles (salvaguardas[48]) seleccionados. Según [5], lo anterior implica una actualización de la valoración del riesgo que considere la eficacia esperada de las salvaguardas seleccionadas. En razón de lo expuesto, resulta necesario estimar la eficacia de las salvaguardas seleccionadas. Lamentablemente, MAGERIT V3 no define ningún criterio para tal fin, impidiendo la determinación del riesgo residual e interrumpiendo la gestión de riesgos de la SI.
Objetivo: definir los criterios para la valoración de las salvaguardas.
Productos de entrada: el esquema usado por PILAR para la determinación de la eficacia de las salvaguardas. Consultar el manual de PILAR [52].
Productos de salida: los criterios para la valoración de las salvaguardas.
Guía: En el apartado A.7, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se suministra una completa orientación en todo lo relacionado con la definición de los criterios para la valoración de las salvaguardas.

Tabla 5.14. Descripción de la actividad MARA 4.1

[48] Cabe recordar que, como se mencionó en el glosario de este documento, los términos "salvaguarda" y "control" son equivalentes y que, por ende, pueden ser usados indistintamente.

MARA.4. Caracterización de las salvaguardas **MARA.4.2. Definir criterios para el tratamiento del riesgo**
Frente a las cuatro opciones de tratamiento disponibles, que se ilustran en la Tabla 2.1, resulta necesario disponer de criterios que permitan tomar decisiones reproducibles, objetivas e imparciales sobre la opción de tratamiento que se ha de aplicar a cada riesgo identificado. Lamentablemente, la metodología MAGERIT V3 no provee ningún criterio para tal fin.
Objetivo: definir los criterios para el tratamiento de los riesgos de SI.
Productos de entrada: las zonas de riesgo y demás lineamientos ofrecidos por la sección 3.1.4 del documento [22].
Productos de salida: los criterios para el tratamiento de los riesgos de SI.
Guía: En el apartado A.6, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se suministra una completa orientación en todo lo relacionado con la definición de los criterios para el tratamiento del riesgo

Tabla 5.15. Descripción de la actividad MARA 4.2

MARA.4. Caracterización de las salvaguardas **MARA.4.3. Identificación de las salvaguardas**
Con esta tarea se pretende identificar las salvaguardas necesarias para tratar los riesgos identificados por las tareas MARA.3. *Estimación del estado del riesgo.* Frente a las cuatro opciones de tratamiento disponibles[49], se deberá usar los criterios obtenidos de la tarea MARA.4.2 con el fin de tomar decisiones reproducibles y objetivas a la hora de seleccionar la opción más adecuada para tratar cada riesgo identificado.
Objetivo: identificar las salvaguardas (controles) necesarias para tratar los riesgos a los que se encuentran expuestos los activos vinculados al caso de estudio
Productos de entrada: los criterios para el tratamiento de riesgos y el *Informe de riesgo potencial,* obtenido de la tarea MARA.3.3
Productos de salida: el Plan de Tratamiento de Riesgos (PTR)[50]
Guía: Primero que todo, se deberá usar los criterios para el tratamiento de riesgos, definidos por la tarea MARA.3.2, con el fin de seleccionar la opción de tratamiento más adecuada para la mitigación de cada riesgo identificado por el *Informe riesgo potencial,* obtenido de la tarea MARA.3.3.

[49] Las cuatro opciones de tratamiento son: modificación, retención, evitación y transferencia. Para mayor información, consultar la Tabla 2.1

[50] MAGERIT V3 lo denomina como *Relación de salvaguardas a desplegar* o *Inventario de salvaguardas*.

Para dar cumplimiento a lo establecido por la cláusula 6.1.3 de la norma ISO/IEC 27001 [2], se recomienda que, para aquellos riesgos que se vayan a tratar mediante la opción de ***reducción***, se seleccionen los controles que se han de implementar para llevar a cabo la reducción de los riesgos, acudiendo, como punto de referencia, a los 114 controles ofrecidos por el Anexo A de la norma ISO/IEC 27001 [2]. Por recomendación del estándar ISO/IEC 27003 [4], el PTR deberá describir claramente: • La relación entre los riesgos y la opción de tratamiento seleccionada para su mitigación • La relación entre los riesgos y los controles seleccionados para implementar la opción de tratamiento seleccionada (especialmente para el caso de la reducción del riesgo) • Las prioridades para el tratamiento de los riesgos. Cabe mencionar que la versión original excluyo todos los productos de entrada definidos por la versión original, pues ésta última estaba generando un incumplimiento a los requerimientos establecidos por la norma ISO/IEC 27001 [2], tal y como se discutió en la sección 2.3.2. En respuesta a ello, esta actividad tuvo que ser replanteada de acuerdo con los lineamientos ofrecidos por el estándar ISO/IEC 27005 [5], el cual establece que solamente se debe considerar el Informe de riesgo potencial, obtenido de la tarea MARA.3.3.

Tabla 5.16. Descripción de la actividad MARA 4.3

MARA.4. Caracterización de las salvaguardas **MARA.4.4. Valoración de las salvaguardas**
Como se discutió en la sección 5.4.1, el estándar ISO/IEC 27005 [5] establece que, una vez definido el PTR, se deberá estimar los riesgos residuales, lo cual implicará una actualización de la valoración del riesgo que considere la eficacia esperada de las salvaguardas seleccionadas. En razón de lo expuesto, resulta necesario valorar las salvaguardas de acuerdo con los criterios definidos por la tarea MARA.4.1.
Objetivo: valorar las salvaguardas seleccionadas y estimar el riesgo residual al que se enfrentarán los activos después de la implementación de las salvaguardas (controles) seleccionadas.
Productos de entrada: los criterios para la valoración de las salvaguardas, el PTR y el *Informe de riesgo potencial,* obtenido de la tarea MARA.3.3
Productos de salida: informe de riesgo residual
Guía: En el apartado A.7, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se suministra una completa orientación en todo lo relacionado con la valoración de las salvaguardas.
Observaciones:

Cabe mencionar que la versión original de esta tarea establecía el producto de salida: *Informe de insuficiencias,* el cual fue excluido de la versión adaptada porque dicho entregable ya fue satisfecho por la sección 4.3.3: *Evaluación del estado actual de la SI*

Tabla 5.17. Descripción de la actividad MARA 4.4

MARA.4. Caracterización de las salvaguardas **MARA.4.5. Aceptación de riesgos**
De acuerdo con el requerimiento establecido por el inciso 6.1.3.f), con esta actividad se pretenderá obtener, formalmente, la aprobación del PTR y la aceptación de los riesgos residuales estimados por la actividad anterior.
Objetivo: Obtener aprobación del PTR y de los riesgos residuales.
Productos de entrada: el *PTR* y el *Informe de riesgo residual* obtenido de la anterior tarea
Productos de salida: la aprobación del PTR, la aceptación de los riesgos y la Declaración de Aplicabilidad (SOA).
Guía: El jefe de División, responsable por la ejecución del caso de estudio, deberá revisar y aprobar el PTR y los riesgos residuales. Se recomienda registrar, en detalle, las condiciones asociadas a tal aprobación.

Tabla 5.18. Descripción de la actividad MARA 4.5

5.3. Guía de recomendaciones sobre la adaptación de MAGERIT V3

La presente guía pretende orientar al usuario sobre cómo debe adaptar la metodología MAGERIT V3 a procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca. Para ello, esta guía le suministra, a quien desee usar la adaptación propuesta, las instrucciones necesarias para la adecuada ejecución de las tareas formalizadas por el Método de Análisis de Riesgos Adaptado –MARA-.

5.3.1. Guía para la clasificación de activos

En el capítulo 2 de la guía [23], se declara que los activos se pueden clasificar en: información, claves criptográficas, servicios, software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones y

personal. Respecto a lo anterior, la norma ISO/IEC 27001 [2], sugiere que la información, a su vez, se clasifique en función de su valor y criticidad con el fin de garantizar que ésta reciba un nivel apropiado de protección de acuerdo con su importancia para la organización[51].

- **Esquema para la clasificación de la información**

En la sección 4.1 del documento [23] se evidencia que MAGERIT V3 reconoce dos opciones para clasificar la información: el esquema nacional de España[52] y el de la Unión Europea[53]. Sin embargo, por obvias razones, ninguno estará alineado con la normativa colombiana, por lo cual resultarán inadecuados para gestionar los riesgos de la SI en procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca.

Como se mencionó en la sección 4.3.2, en Colombia, por orden del artículo 5 de la ley 1712 de 2014[54] [41], las entidades públicas como la Universidad del Cauca adquieren la calidad de *sujetos obligados* y, por ende, toda la información que gestionen será objeto de las disposiciones estipuladas por dicha ley, cuyo artículo 6 establece que la información puede tomar tres formas como lo muestra, a continuación, la Tabla 5.19[55].

Categoría	Definición	Ejemplos	Relación con la ley de Hábeas Data
Información Pública Reservada	La ley 1712 de 2014 la define como: "aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos	Toda información que por mandato legal tiene reserva legal. Por ejemplo: reserva médica, reserva bancaria, reserva legal. Datos personales sensibles que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, tales como aquellos que revelan el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, a organizaciones	Este tipo de información corresponde a los datos que la ley de Hábeas Data califica como privados y que además son exceptuados a la ciudadanía por daños a intereses públicos

[51] Ver el control A.8.2 que sugiere la norma ISO/IEC 27001 [2] en su Anexo A.
[52] Define 5 categorías: Secreta, Reservada, Confidencial, Difusión Limitada y Sin Clasificar.
[53] Define 4 categorías: TRES SECRET UE, SECRET UE, CONFIDENTIEL UE, RESTREINT UE.
[54] Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
[55] Los ejemplos expuestos por la Tabla 5.19 fueron tomados de [42]

	consagrados en el artículo 19 de esta ley". Compuesta por información personal, estrechamente relacionada con los derechos fundamentales del titular: dignidad, intimidad y libertad, por lo que "se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en cumplimiento de sus funciones.	sociales, así como los datos relativos a la salud, la vida sexual, Información genética y los datos biométricos. Toda información exceptuada de acceso a la ciudadanía por daño a los intereses públicos, como la información de defensa, seguridad nacional y de seguridad pública. La información que afecte la administración efectiva de la justicia o las relaciones internacionales. La información que sirva para la prevención, investigación y persecución de los delitos y las faltas disciplinarias	
Información pública clasificada	De acuerdo a la ley 1712 de 2014 se define como "aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los	Toda información que pertenece al ámbito propio, particular, privado o semiprivado de una persona natural o jurídica. Los datos personales de las hojas de vida que no son públicos. Libros de comerciantes e historias clínicas Documentos que contengan información personal. Por ejemplo: número de cuenta de ahorros, dirección de residencia, teléfonos personales, datos de núcleo familiar. Datos relativos a las relaciones con entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas	Este tipo de información incluye a los datos que la ley de Hábeas Data denomina como privados o semi-privados.

	derechos particulares o privados consagrados en el artículo 18 de esta ley".		
Información Pública	De acuerdo a la ley 1712 de 2014 se define como: "aquella que puede ser obtenida y ofrecida sin reserva alguna. Esta información es creada en el curso normal de la función misional de la entidad y tiene poca probabilidad de causar daño.	Ofertas de cargos en el sector oficial. Actas de adjudicación de contratos. Datos sobre el estado civil de las personas o sobre la conformación de la familia. Demás información que la organización considere de carácter público.	Este tipo de información incluye los datos que la ley de Hábeas Data denomina como públicos

Tabla 5.19. Categorías de la información según [41]

Cabe mencionar que este esquema de clasificación fue identificado gracias al documento [42], el cual fue elaborado por la Presidencia de la República de Colombia. La relevante y prestigiosa procedencia de [42] justifica y valida la formulación de esta adaptación que se sugiere usar durante la gestión de riesgos de SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca.

- **Clasificación de los demás activos**

Para clasificar los demás activos, que no sean información, se recomienda seguir la tipificación que MAGERIT V3 define en el capítulo 2 del documento [23]. Esta es ilustrada, a continuación, por la Tabla 5.20.

Tipo de activo	Descripción
Servicios	Función que satisface una necesidad de los usuarios.
Claves criptográficas	Es una pieza de información que controla la operación de un algoritmo criptográfico y se emplean para proteger el secreto o autenticar a las partes.

Software -	Soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios para realizar ciertas tareas.
Hardware	Se refiere a cualquiera de las partes físicas de un sistema informático.
Redes de comunicaciones	Hace referencia a todo activo que proporcione la capacidad y los elementos necesarios para mantener un intercambio de información digital.
Soportes de información	Hace referencia a los dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
Equipamiento auxiliar	Hace referencia a los activos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Instalaciones	Hace referencia a los recintos, bodegas, oficinas y demás ubicaciones físicas que hospeden activos vinculados a la ejecución de las actividades del caso de estudio
Personal	Hace referencia a las personas que intervienen en la ejecución de las actividades del caso de estudio.

Tabla 5.20. Tipificación de activos que no sean información. Tomada de [41]

Para más detalles acerca de la clasificación de activos, que no sean de tipo información, remitirse al capítulo 2 del documento [23].

5.3.2. Organización para operar la gestión de riesgos

Para la gestión de riesgos de SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca, se sugiere no usar la matriz de asignación de responsabilidades que MAGERIT V3 propone en la sección 4.2.1 del documento [22], pues como lo afirma [22], ésta solo es orientativa y cada organización deberá ajustarla a sus necesidades particulares.

En lugar de ello, se sugiere considerar la Tabla 3.1, en la cual se definen los roles de SI con base en la estructura organizacional de la Universidad del Cauca, sus órganos directivos y dependencias, asignando claramente las responsabilidades frente a la operación de la gestión de riesgos y demás actividades de la SI.

5.3.3. Guía para la valoración de activos

- **Definición de los criterios**

En [22], MAGERIT V3 manifiesta que la valoración no debe centrarse en el costo de adquisición o reposición de los activos, sino más bien en la importancia que estos tienen para la organización y en el nivel de protección que requieren. Por ende, resulta necesario definir criterios para valorar los activos en términos de su importancia para la Universidad del Cauca y de las consecuencias que se pueden desencadenar en caso de que éstos se vean comprometidos.

Respecto a lo anterior, el Centro Criptológico Nacional de España, en el marco del Esquema Nacional de Seguridad, sugiere, mediante la guía CCN-STIC-803 [50], un amplio conjunto de criterios que deberán ser adaptados al contexto normativo establecido por las leyes colombianas con el fin de adecuarlos al caso de estudio. Consecuentemente, surge la necesidad de agregar nuevos criterios para garantizar que la valoración de los activos esté alineada con el contexto normativo en el que se ejecutan los procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca.

Adicionalmente, se recomienda ajustar la escala que MAGERIT V3 ofrece en [23], para redefinir tres niveles que no resultan claramente diferenciables: "*alto*", "*muy alto"* y "*extremo".* De esta manera se evitarán esfuerzos innecesarios en intentos por discernir entre estas categorías*.* El resultado de esta adaptación se muestra, a continuación, por la escala ilustrada por la Tabla 5.21

Valor del Activo	
9-10	Muy Alto
6-8	Alto
3-5	Medio
1-2	Bajo
0	Despreciable

Tabla 5.21. Escala para la valoración de los activos

En virtud de lo señalado, para la gestión de riesgos de la SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca, se aconseja considerar la escala ilustrada por la Tabla 5.21 y de igual manera se recomienda agregar los siguientes criterios:

a. Criterios para valorar la confidencialidad de la información con base en la clasificación dictada por el artículo 6 de la ley 1712 de 2014 [41].

    - La **Información Pública Reservada** obtendrá un valor de 10/10 (MUY ALTO) en su dimensión de confidencialidad.

- La **Información Pública Clasificada** obtendrá un valor de 8/10 (ALTO) en su dimensión de confidencialidad.

- La **Información Pública** obtendrá un valor de 3/10 (MEDIO) en su dimensión de confidencialidad.

b. Criterios para valorar los activos en términos del grado del incumplimiento, del derecho del Habeas Data y de la ley Protección de Datos Personales, que se podría generar en caso de que los activos se vean comprometidos. Considerando dichas leyes y la severidad de las sanciones que en ellas se estipulan[56], se proponen los siguientes criterios:

- Obtendrá una valoración de 10/10 (MUY ALTO), en la dimensión que corresponda, todo activo que, al verse comprometido, cause un **grave incumplimiento** del derecho del Habeas Data o de la ley de Protección de Datos Personales.

- Obtendrá una valoración de 8/10 (ALTO), en la dimensión que corresponda, todo activo que, al verse comprometido, cause **cierto incumplimiento** del derecho del Habeas Data o de la ley de Protección de Datos Personales.

- Obtendrá una valoración de 5/10 (MEDIO), en la dimensión que corresponda, todo activo que, al verse comprometido, cause un **leve incumplimiento** del derecho del Habeas Data o de la ley de Protección de Datos Personales.

Con estos criterios se logrará alinear la valoración de los activos con las disposiciones emanadas por la ley colombiana para la protección de datos personales[57] y la ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional[58]. También se aconseja adicionar todos los criterios que se consideren necesarios para ajustar este enfoque al contexto del procedimiento sobre el cual se pretenda gestionar los riesgos de la SI.

Adicionalmente, fue necesario adecuar los enunciados de los criterios, inicialmente ofrecidos por el Centro Criptológico Nacional de España, para que fueran más comprensibles a los ojos de los propietarios de los activos, incluyendo un lenguaje familiar con la jerga característica del contexto del caso de estudio. Lo anterior con el

[56] Las sanciones podrían llegar a causar el cierre o clausura total de las operaciones del caso de estudio.
[57] Ley estatutaria 1581 de 2012 [37]
[58] Ley 1712 de 2014 [41]

fin de garantizar una correcta comprensión y aplicación de los criterios para lograr la mayor precisión posible a la hora de valorar los activos.

Como resultado de estas adaptaciones, se obtuvo el conjunto de criterios que la presente guía recomienda usar para valorar los activos en el marco de la gestión de riesgos de SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca. Dichos criterios son expuestos, a continuación, por la Tabla 5.22.

Tipo de Criterio	**ID**	**VALOR**	**CRITERIO**
Clasificación de la información	10.ci	10	INFORMACION PUBLICA RESERVADA
	8.ci	8	INFORMACION PUBLICA CLASIFICADA
	2.ci	2	INFORMACION PUBLICA
Información Personal	9.ip	9	puede afectar gravemente a un grupo de individuos
	8.ip	8	puede afectar gravemente a un individuo
	7.ip	7	puede afectar a un grupo de individuos
	6.ip	6	puede afectar a un individuo
	5.ip	5	puede afectar levemente a un grupo de individuos
	4.ip	4	puede afectar levemente a un individuo
Seguridad	10.s.a	10 (a)	puede causar un incidente de seguridad excepcionalmente grave o puede dificultar la investigación de los mismos
	10.s.b	10 (b)	puede facilitar la comisión de delitos excepcionalmente graves o puede dificultar la investigación de los mismos
	9.s.a	9 (a)	puede causar un grave incidente de seguridad o puede dificultar la investigación de los mismos
	9.s.b	9 (b)	puede facilitar la comisión de delitos graves o puede dificultar la investigación de los mismos
	7.s.a	7 (a)	puede causar un incidente de seguridad o puede dificultar la investigación de los mismos
	7.s.b	7 (b)	puede facilitar la comisión de delitos o puede dificultar la investigación de los mismos
	5.s.a	5 (a)	puede causar un incidente leve de seguridad o puede dificultar la investigación de los mismos
	5.s.b	5 (b)	puede facilitar la comisión de delitos leves o puede dificultar la investigación de los mismos
Interrupción de las actividades	9.iap.a	9 (a)	puede causar una interrupción excepcionalmente grave de las actividades del procedimiento

del procedimiento	9.iap.b	9 (b)	puede causar una interrupción excepcionalmente grave de las actividades en otras dependencias de la Universidad o en organizaciones externas
	7.iap.a	7 (a)	puede causar una interrupción grave de las actividades del procedimiento
	7.iap.b	7 (b)	puede causar una interrupción grave de las actividades en otras dependencias de la Universidad o en organizaciones externas
	5.iap.a	5 (a)	puede causar una interrupción de las actividades del procedimiento
	5.iap.b	5 (b)	puede causar una interrupción de las actividades en otras dependencias de la Universidad o en organizaciones externas
	3.iap.a	3 (a)	Puede causar una leve interrupción de las actividades del procedimiento.
	3.iap.b	3 (b)	puede causar una leve interrupción de las actividades en otras dependencias de la Universidad o en organizaciones externas
Pérdida de Confianza (Reputación)	9.rep.a	9 (a)	puede generarle, al procedimiento, una publicidad negativa por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones
	9.rep.b	9 (b)	puede generarle, al procedimiento, una publicidad negativa por afectar de forma excepcionalmente grave a las relaciones con la comunidad universitaria
	7.rep.a	7 (a)	puede generarle, al procedimiento, una publicidad negativa por afectar gravemente a las relaciones con otras organizaciones
	7.rep.b	7 (b)	puede generarle, al procedimiento, una publicidad negativa por afectar gravemente a las relaciones con la comunidad universitaria
	5.rep.a	5 (a)	puede generarle, al procedimiento, una publicidad negativa por afectar a las relaciones con otras organizaciones
	5.rep.b	5 (b)	puede generarle, al procedimiento, una publicidad negativa por afectar a las relaciones con la comunidad universitaria
Intereses Comerciales / Económicos	9.ic.a	9 (a)	De elevado valor comercial
	9.ic.b	9 (b)	Puede causar pérdidas económicas elevadas (disminución elevada de ingresos)
	9.ic.c	9 (c)	Puede proporcionar elevadas ganancias o ventajas a individuos u organizaciones

	9.ic.d	9 (d)	Constituye un incumplimiento grave de las obligaciones contractuales adquiridas con las entidades que financian los proyectos de investigación
	7.ic.a	7 (a)	De cierto valor comercial
	7.ic.b	7 (b)	Puede causar pérdidas económicas (o disminución de ingresos)
	7.ic.c	7 (c)	Puede proporcionar ganancias o ventajas a individuos u organizaciones
	7.ic.d	7 (d)	Constituye un incumplimiento de las obligaciones contractuales adquiridas con las entidades que financian los proyectos de investigación
	3.ic.a	3 (a)	De bajo valor comercial
	3.ic.b	3 (b)	Puede causar leves pérdidas económicas (o disminución leve de ingresos)
	3.ic.c	3 (c)	Puede proporcionar leves ganancias o ventajas a individuos u organizaciones
Operaciones	10.ope	10	puede causar una disminución excepcionalmente alta de la eficacia del procedimiento, entorpeciendo la consecución de sus objetivos
	9.ope	9	puede causar una alta disminución de la eficacia del procedimiento, entorpeciendo la consecución de sus objetivos
	7.ope	7	puede causar una disminución de la eficacia del procedimiento, entorpeciendo la consecución de sus objetivos
	5.ope	5	puede causar una leve disminución de la eficacia del procedimiento, entorpeciendo la consecución de sus objetivos
Orden Público	9.op	9	puede alterar seriamente el orden público
	6.op	6	puede causar manifestaciones, o presiones significativas
	3.op	3	puede causar protestas puntuales
Tiempo de Recuperación del Servicio	9.trs	9	El servicio deberá restablecerse en un periodo de tiempo no mayor a 4 horas
	6.trs	6	El servicio deberá restablecerse en un periodo de tiempo no mayor a 1 día
	3.trs	3	El servicio deberá restablecerse en un periodo de tiempo no mayor a 5 días

Tabla 5.22. Criterios para la valoración de activos. Basada en [23]

- **Cargando PILAR con los criterios propuestos**

Para equipar a PILAR con este conjunto de criterios propuestos y lograr, de esa manera, aprovechar todos los beneficios que se pueden obtener al usar esta herramienta durante la valoración de los activos, se deberán seguir los pasos que se listan a continuación:

1. Cerrar PILAR
2. Descargar el archivo [54].
3. Entrar a la carpeta **bib_es** ubicada en el directorio de instalación de PILAR[59].
4. Reemplazar el archivo **criteria_es.xml** por [54].
5. Ejecutar la herramienta PILAR

Después de seguir estos pasos, se logrará que la herramienta PILAR cargue y use los criterios expuestos por la Tabla 5.22, ofreciendo una adecuada valoración de activos que se ajusta al contexto de los procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca.

Cabe mencionar que, en caso de que se requiera agregar nuevos criterios o ajustar los ya existentes, se deberá modificar el archivo [54], teniendo en cuenta las instrucciones impartidas por la sección 4.2.1 del documento [23].

- **Corrección de fallas**

Durante la cuarta etapa de desarrollo del proyecto y mientras se ejercitaba la adaptación propuesta a la metodología MAGERIT V3, la sección 6.1.1 permitió identificar algunas fallas de la presente guía en cuanto a la valoración de los activos, dando origen a la necesidad de formular nuevas adaptaciones. Como resultado se generaron algunas recomendaciones adicionales como se discute a continuación:

<u>En cuanto a los activos que se deben valorar</u>

MAGERIT V3 manifiesta que el valor nuclear suele estar en los activos esenciales que, como se mencionó anteriormente, corresponden a la información gestionada y los servicios que se prestan, quedando los demás activos subordinados a las necesidades de protección de lo esencial. Según MAGERIT V3, todo activo que no sea de tipo información o servicios no necesitará que se le asigne valor propio, pues éstos resultarán valiosos en la medida en que soporten los activos esenciales.

En virtud de lo señalado, se recomienda que, para la gestión de riesgos de la SI, aplicando la metodología MAGERIT V3, para procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca, se valoren únicamente los activos esenciales y dejar que el valor de los demás activos lo determine,

[59] Por defecto, el directorio de instalación de PILAR será: C:\Program Files (x86)\PILAR_5.4\

automáticamente, la herramienta PILAR como el acumulado de los valores que éstos heredan de sus superiores a través de las dependencias.

En cuanto a las dimensiones que se deben valorar

En [22], MAGERIT V3 propone valorar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, no obstante, las únicas dimensiones que la norma ISO/IEC 27001 [2] exige tener en cuenta son la confidencialidad, integridad y la disponibilidad. Además, en [22] MAGERIT V3 manifiesta que la autenticidad y la trazabilidad fueron añadidas como dimensiones complementarias encaminadas a mantener la integridad y la confidencialidad.

En razón de lo expuesto, se recomienda que, para la gestión de riesgos de la SI, aplicando la metodología MAGERIT V3, para procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca, solamente se valoren las tres dimensiones primarias de los activos: confidencialidad, integridad y disponibilidad.

Finalmente, para valorar las dimensiones primarias de cada activo con la ayuda de PILAR y con base en los criterios expuestos por la Tabla 5.22, resulta necesario preguntarse:

- En cuanto a la confidencialidad: ¿qué daño causaría que el activo sea conocido por quien no debe? ¿Qué consecuencias traería la divulgación de información que no sea pública? Luego de pensar en las posibles consecuencias, se deberá seleccionar, en PILAR, los criterios que se cumplen si la confidencialidad del activo se ve comprometida. PILAR calculará el valor de esta dimensión como el mayor valor de los criterios seleccionados.

- En cuanto a la integridad: ¿qué perjuicio causaría que el activo estuviese dañado o corrupto? Esta valoración es típica de los datos, los cuales pueden ser manipulados, ser total o parcialmente falsos o, incluso, estar incompletos. Luego de pensar en las posibles consecuencias, se deberá seleccionar, en PILAR, los criterios que se cumplen si la integridad del activo se ve comprometida. PILAR calculará el valor de esta dimensión como el mayor valor de los criterios seleccionados.

- En cuanto a la disponibilidad: ¿qué perjuicio causaría no tener el activo, o no poder utilizarlo? Luego de pensar en las posibles consecuencias, se deberá seleccionar, en PILAR, los criterios que se cumplen si la disponibilidad del activo se ve comprometida. PILAR calculará el valor de esta dimensión como el mayor valor de los criterios seleccionados.

5.3.4. Guía para la valoración de las amenazas

- **Definición de los criterios**

En [22], MAGERIT V3 declara que para poder valorar la influencia que una amenaza tiene sobre el valor de los activos, se deberá determinar su probabilidad de ocurrencia y la degradación que ésta pueda llegar causar. El estándar ISO/IEC 27005 [5] recomienda desarrollar criterios que permitan realizar las valoraciones de manera objetiva y reproducible, sin embargo, MAGERIT V3 no dispone de ellos, pese a las sugerencias del estándar.

Respecto a lo anterior, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos - NIST[60], encargado de promover la innovación y competencia industrial en Estados Unidos, publicó el documento [51], en el cual se provee una sólida guía para la gestión de riesgos que incluye un conjunto de criterios para valorar la probabilidad de ocurrencia de las amenazas y la degradación que éstas pueden causar sobre los activos.

En razón de lo expuesto, se recomienda complementar el vacío que tiene MAGERIT V3, debido a su carencia de criterios para la valoración de amenazas, con lo aportado por NIST en su publicación especial [51]. Cabe mencionar que, como se explica a continuación, los criterios propuestos por NIST resultaron ser completamente compatibles con la metodología MAGERIT V3 e interoperables con PILAR, permitiendo sacarle el mayor provecho a esta herramienta de apoyo.

Criterios para valorar la probabilidad de ocurrencia de una amenaza.

Gracias a las afirmaciones del capítulo 2 del documento [24] y a la tabla de frecuencias definidas en la sección 4.2 del manual [47], se logró identificar que MAGERIT V3 mide la probabilidad en términos de la tasa de ocurrencia anual, de la misma manera como lo hace NIST. Consecuentemente, resulta válido afirmar que los criterios definidos por NIST son completamente compatibles con MAGERIT V3 y, mejor aún, que sus resultados podrán ser procesados por PILAR mediante un simple mapeo de valores, permitiendo sacar el mayor provecho a esta herramienta de apoyo.

En razón de lo expuesto, se recomienda que, para la gestión de riesgos de la SI, aplicando la metodología MAGERIT V3, en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca, se adopten los criterios que NIST propone para la valoración de la probabilidad de ocurrencia de las amenazas. Dichos criterios son discutidos a continuación.

[60] Por sus siglas en inglés: National Institute of Standards and Technology

En [51], NIST declara que para poder determinar la probabilidad de que una amenaza se materialice sobre un activo, se deberá identificar, primero:

a. La probabilidad de que la amenaza se materialice sin intervención alguna. Para su determinación, NIST define los siguientes criterios:

Valor NIST		Mapeo de valores a PILAR	Descripción
10	Muy Alta	**CS** (Casi seguro)	Es casi seguro (sucede más de 100 veces al año).
8	Alta	**MA** (Muy Alta)	Es altamente probable (sucede entre 10-100 veces al año).
5	Media	**P** (Posible)	Es algo probable (sucede de 1 a 10 veces al año).
2	Baja	**PP** (Poco probable)	Es improbable (sucede menos de una vez al año, pero más de una vez cada 10 años).
0	Muy Baja	**MR** (Muy Rara)	Es altamente improbable (sucede menos de una vez cada 10 años.)

Tabla 5.23 Criterios para determinar la probabilidad de que la amenaza se materialice sin intervención. Tomada de [51]

b. Probabilidad de que un atacante materialice la amenaza. Para su determinación, NIST define los siguientes criterios:

Valor NIST		Mapeo de valores a PILAR	Descripción
10	Muy Alta	**CS** (Casi seguro)	Es casi seguro que un atacante logre materializar la amenaza.
8	Alta	**MA** (Muy Alta)	Es altamente probable que un atacante logre materializar la amenaza.
5	Media	**P** (Posible)	Es algo probable que el atacante logre materializar la amenaza.
2	Baja	**PP** (Poco probable)	Es improbable que el atacante logre materializar la amenaza.

0	Muy Baja	**MR** (Muy Rara)	Es altamente improbable que el atacante logre materializar la amenaza.

Tabla 5.24 Criterios para determinar la probabilidad de que un atacante materialice la amenaza. Tomada de [51]

c. Motivación e intereses del atacante sobre la materialización de la amenaza:

Valor de la probabilidad		**Descripción**
10	**CS** (Casi seguro)	Si logra materializar la amenaza, el atacante obtendrá enormes beneficios económicos y reconocimientos por parte de la comunidad.
8	**MA** (Muy Alta)	Si logra materializar la amenaza, el atacante obtendrá beneficios económicos y/o reconocimientos por parte de la comunidad.
5	**P** (Posible)	Si logra materializar la amenaza, el atacante obtendrá ciertos beneficios económicos.
2	**PP** (Poco probable)	Si logra materializar la amenaza, el atacante beneficiará su estima u obtendrá cierto reconocimiento por parte de la comunidad.

Tabla 5.25 Criterios para determinar los intereses de un atacante.

d. Probabilidad de que la materialización de la amenaza resulte en impactos adversos para la organización. Para su determinación, NIST define los siguientes criterios:

Valor NIST		**Mapeo de valores a PILAR**	**Descripción**
10	Muy Alta	**CS** (Casi seguro)	Es casi seguro que haya impactos adversos.
8	Alta	**MA** (Muy Alta)	Es altamente probable que haya impactos adversos.
5	Media	**P** (Posible)	Es algo probable que haya impactos adversos.
2	Baja	**PP** (Poco probable)	Es improbable que haya impactos adversos.

0	Muy Baja	**MR** (Muy Rara)	Es altamente improbable que haya impactos adversos.

Tabla 5.26 Criterios para determinar la probabilidad de que la amenaza resulte en impactos adversos. Tomada de [51]

Una vez valorados los tres aspectos mencionados anteriormente, se puede calcular el valor final de la probabilidad de ocurrencia de la amenaza, para lo cual, se provee la siguiente matriz:

Mayor valor seleccionado entre los criterios de las Tablas 5.23, 5.24, 5.25	**Probabilidad de que la materialización termine en impactos adversos – valor de los criterios Tabla 5.26**				
	MR	**PP**	**P**	**MA**	**CS**
CS	PP	P	MA	CS	CS
MA	PP	P	P	MA	CS
P	PP	PP	P	P	MA
PP	MR	PP	PP	P	P
MR	MR	MR	PP	PP	PP

Tabla 5.27. Matriz para el cálculo de la probabilidad de ocurrencia de una amenaza. Tomada de [51]

Criterios para valorar la degradación que puede causar una amenaza

Gracias a [24, 47] se logra identificar que tanto MAGERIT V3 como PILAR determinan la degradación como un valor entre 0 y 100, indicando el porcentaje del valor que pierden los activos a causa de las amenazas, de la misma manera como lo propone NIST en su publicación especial [51]. Lo anterior hace posible el uso del aporte de NIST como complemento a la metodología MAGERIT V3, permitiendo, además, usar los resultados en conjunto con la herramienta PILAR.

En razón de lo expuesto, se recomienda que, para la gestión de riesgos de la SI, aplicando la metodología MAGERIT V3, en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca, se adopten los criterios definidos por NIST para la valoración de la degradación que pueden causar las amenazas. Dichos criterios son expuestos, a continuación, por la Tabla 5.28

Valor de la degradación		Significado
96%-100%	Muy alta	La materialización de la amenaza puede tener **múltiples** efectos severos o catastróficos sobre las operaciones de la organización, un activo en particular u otras organizaciones.
80%-95%	Alta	La materialización de la amenaza puede tener un efecto severo o catastrófico sobre las operaciones de la organización, un activo en particular u otras organizaciones. Esto significa que la amenaza podría, por ejemplo: • Causar una degradación sobre el(los) activo(s) tan severa como para impedir que la organización ejecute sus funciones primarias • Causar pérdidas financieras elevadas • Causar daños severos o catastróficos al personal que podrían ocasionar pérdida de vidas.
21%-79%	Media	La materialización de la amenaza puede tener efectos sobre las operaciones de la organización, un activo en particular u otras organizaciones. Esto significa que la amenaza podría, por ejemplo: • Causar una significante degradación sobre el(los) activo(s) que puede reducir la capacidad de la organización para ejecutar sus funciones primarias. • Causar pérdidas financieras. • Causar daños al personal no tan graves como para ocasionar la pérdida de vidas.
5%-20%	Baja	La materialización de la amenaza puede tener leves efectos sobre las operaciones de la organización, un activo en particular u otras organizaciones. Esto significa que la amenaza podría, por ejemplo: • Causar una ligera degradación sobre el(los) activo(s) que puede reducir levemente la capacidad de la organización para ejecutar sus funciones primarias. • Causar pérdidas financieras mínimas.
1%-4%	Despreciable	La materialización de la amenaza puede causar efectos despreciables sobre las operaciones de la organización, un activo en particular u otras organizaciones.

Tabla 5.28. Criterios para valorar la degradación de una amenaza. Tomada de [51]

❖ **Corrección de las fallas**

Durante la cuarta etapa de desarrollo del proyecto y mientras se ejercitaba la adaptación propuesta a la metodología MAGERIT V3, la sección 6.1.2 permitieron identificar algunas fallas en la presente guía en cuanto a la valoración de las amenazas, dando origen a la necesidad de formular nuevas adaptaciones. Como resultado se generaron algunas recomendaciones adicionales como se discute a continuación:

Primero que todo, se sugiere que, para la gestión de riesgos de la SI, aplicando la metodología MAGERIT V3, en procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca, se identifiquen solamente las amenazas que atenten contra los activos no esenciales. En [22], MAGERIT V3 afirma que las amenazas no suelen materializarse sobre los activos esenciales sino, más bien, en los activos que los soportan, propagando su degradación, hacia los primeros, a través de las dependencias existentes. Por ese motivo, se considera totalmente innecesario intentar identificar amenazas sobre los activos esenciales.

Finalmente, en la sección 8.6 del documento [22], MAGERIT V3 manifiesta que determinar la probabilidad de ocurrencia de las amenazas y la degradación causada sobre cada activo, en cada dimensión, es una tarea desmoralizadora, por lo cual sugiere partir de datos estándar que han de ser ajustados hasta reflejar, con la mayor precisión posible, la realidad del caso de estudio. Por la amplia trayectoria, uso y reconocimiento de PILAR, se recomienda que, para la gestión de riesgos de la SI, aplicando la metodología MAGERIT V3, en procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca, se valoren las amenazas tomando, como punto de partida, los datos estándar ofrecidos por la biblioteca que provee la herramienta PILAR.

Como lo afirma la sección 6.1.2, los criterios propuestos, anteriormente en la sección 5.3.4, serán de gran ayuda para ajustar los valores de las amenazas, suministrados por PILAR, a las particularidades del contexto del caso de estudio como el nivel de conciencia y conocimiento en materia de la SI por parte del personal, a las condiciones climáticas de Popayán[61] y a las frecuentes interrupciones del suministro de energía a causa de las tormentas eléctricas, etc. De igual manera, serán útiles cuando se valoren amenazas desconocidas por la biblioteca de datos de PILAR.

5.3.5. Guía para la evaluación del riesgo

La cláusula 6.1.2 de la norma ISO/IEC 27001 [2] establece que los riesgos deben ser evaluados a fin de identificar las prioridades para el tratamiento de los

[61] Por ejemplo, en la ciudad de Popayán se puede presentar una mayor probabilidad de que se materialicen amenazas como las inundaciones.

mismos. Respecto a lo anterior, el estándar ISO/IEC 27005 [2] sugiere desarrollar criterios que permitan evaluar el riesgo de manera objetiva y reproducible, sin embargo, MAGERIT V3 no dispone de ellos, pese a las sugerencias del estándar.

En razón de lo expuesto, resulta necesario definir criterios que, estando alineados con el contexto del caso de estudio, permitan evaluar los riesgos de manera objetiva y reproducible. Para ello, se deberá contar con una escala que represente el valor del riesgo, sin embargo MAGERIT V3 no define nada que se le parezca.

Según [47], PILAR utiliza una escala discreta de valores entre 0 y 9 para representar los niveles de riesgo, como la ilustrada por la Tabla 5.29, de la cual se evidencia una notoria ambigüedad entre los niveles: *Extremadamente crítico, Muy crítico, Crítico, Muy alto,* y *Alto*. Para evitar esfuerzos innecesarios en intentos por discernir entre estas categorías, se considera conveniente usar la escala ilustrada por la Tabla 5.30.

Valor del riesgo	Significado
7 o más	Extremadamente crítico
6	Muy crítico
5	Crítico
4	Muy alto
3	Alto
2	Medio
1	Bajo

Tabla 5.29. Escala del nivel de riesgo definida en [47]

Valor del riesgo	Significado
5 o más	Crítico
3,6 – 4,9	Alto
2,0 – 3,5	Medio
1,0 - 1,9	Bajo
0 - 0,9	Despreciable

Tabla 5.30. Escala del nivel de riesgo

Con base en lo anterior, el nivel de riesgo estará compuesto por tres valores, cada uno representando el riesgo en cada dimensión de los activos: confidencialidad, disponibilidad e integridad. Tener tres valores, en lugar de uno, dificulta la aplicación de los criterios para la evaluación de los riesgos y sus respectivos umbrales. Frente a ello, y por recomendación de un experto en la SI[62], se propone calcular la media ponderada de los riesgos estimados en cada una de las tres dimensiones y considerar dicho valor en lugar de los tres por separado.

Considerando el énfasis que hacen las leyes 1712 de 2014 [41], 1266 de 2008 [36] y 1581 de 2012 [37] por la protección de la confidencialidad de la información, se propone distribuir el peso de los riesgos según la dimensión afectada, como lo ilustra, a continuación, la Tabla 5.31.

[62] Especialista en redes y servicios telemáticos Siler Amador Donado

DIMENSIÓN AFECTADA	PESO
Confidencialidad	40%
Disponibilidad	30%
Integridad	30%

Tabla 5.31 Peso del riesgo según la dimensión afectada

Una vez obtenido el valor ponderado, se puede proceder con la evaluación de los riesgos de SI, no obstante la metodología MAGERIT V3 carece de cualquier criterio para tal fin, pese a las recomendaciones del estándar ISO/IEC 27005 [5]. Para dar solución a este inconveniente, se recomienda usar los criterios propuestos por la Tabla 5.32 para llevar a cabo la definición de las prioridades para el tratamiento. De este modo, se logrará satisfacer el requerimiento emanado por la cláusula 6.1.2 de la norma ISO/IEC 27001 [2].

PRIORIDAD	CRITERIO
Muy Alta	Todo riesgo que comprometa uno o más activos relacionados directamente con los activos esenciales, **especialmente:** el Sistema de Información de la Vicerrectoría de Investigaciones (SIVRI) y el Sistema de Archivo de la VRI: *Satélite*.
Alta	Todo riesgo que comprometa uno o más activos de los cuales SIVRI o Satélite dependa totalmente en las dimensiones relacionadas.
Media	Todo riesgo cuyo valor ponderado sea superior al nivel Bajo, según la escala ilustrada por la Tabla 5.30.
Baja	Cualquier riesgo cuyo valor ponderado este en el nivel *Bajo,* según la escala ilustrada por la Tabla 5.30, tendrá la menor prioridad, mientras que aquellos se encuentren en el nivel despreciable serán excluidos del tratamiento.

Tabla 5.32. Criterios para la evaluación de riesgos

Cabe mencionar que los criterios para la evaluación del riesgo, aquí propuestos, fueron definidos a la medida del caso de estudio, por lo cual existe la posibilidad de que el procedimiento, al cual se le vaya a gestionar los riesgos, difiera lo suficiente como para que se necesiten unos ajustes a los criterios. En ese caso, se recomienda:

- Definir una jerarquía que ordene los activos del procedimiento sobre el cual se van a gestionar los riesgos de la SI, dejando siempre los activos esenciales en la cima y ubicando, en los niveles inferiores, la cadena de activos que los soportan.

- Asignar la mayor prioridad a los riesgos que atenten contra los activos esenciales del procedimiento en cuestión.
- Asignar el siguiente nivel de prioridad a los riesgos que atenten contra los activos que soportan los activos esenciales.
- Asignar al riesgo una prioridad menor de acuerdo a la ubicación jerárquica del activo que se vea afectado.
- Siempre otorgar la menor prioridad a los riesgos cuyo valor ponderado esté en el nivel bajo, de acuerdo con la escala ilustrada por la Tabla 5.30.
- Excluir del tratamiento a todo riesgo cuyo valor ponderado se encuentre en el nivel *Despreciable*, de acuerdo con la escala ilustrada por la Tabla 5.30.

5.3.6. Guía para el tratamiento del riesgo

Frente a las cuatro opciones de tratamiento disponibles, que se ilustran en la Tabla 2.1, resulta necesario disponer de criterios que permitan tomar decisiones reproducibles, objetivas e imparciales sobre la opción de tratamiento que se ha de aplicar a cada riesgo identificado. Lamentablemente, la metodología MAGERIT V3 no provee ningún criterio para tal fin.

En respuesta a lo anterior, en la sección 4.1.3 del documento [22], MAGERIT V3 define cuatro zonas de riesgo, ilustradas por la Figura 5.3, para las cuales se proponen las opciones de tratamiento aplicables con base en los lineamientos ofrecidos por la guía que elaboró el Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia [53] y teniendo en cuenta la escala del nivel de riesgo ilustrada por la Tabla 5.30. Como resultado se obtiene:

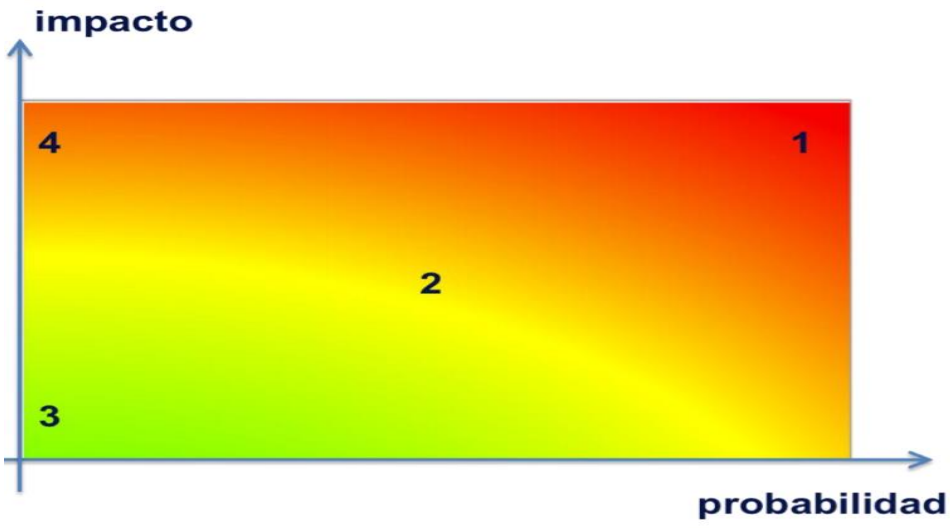

Figura 5.3. Zonas de riesgo. Tomada de [22]

- Zona 1: Riesgos altos-críticos que se caracterizan por ser muy probables y de muy alto impacto. Todo riesgo cuyo valor estimado sea mayor a 3,5 pertenecerá a esta zona y las opciones de tratamiento aplicables serán: modificación, transferencia y evitación.

- Zona 2: Agrupa los riesgos de nivel medio incluyendo un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo. Todo riesgo cuyo valor estimado esté entre 2,0 y 3,5 pertenecerá a esta zona. Las opciones de tratamiento aplicables son: retención, modificación y transferencia.

- Zona 3: representa el nivel de riesgo aceptable, por lo cual, la única opción de tratamiento aplicable es la retención. El responsable del caso de estudio[63] define que el nivel de riesgo aceptado será *Bajo*. En razón de lo expuesto, a esta zona pertenecerán todos los riesgos cuyo valor estimado esté entre 1,0 y 1,9.

- Zona 4: Agrupa los riesgos que, a pesar de tener un valor estimado *Bajo*, no deberían ser retenidos por su alto impacto a los activos. Para esta zona las opciones de tratamiento aplicables son: modificación, transferencia y evitación.

Como la metodología MAGERIT V3 no define ningún criterio para el tratamiento de riesgos, se recomienda que, con base en estas zonas y considerando la escala ilustrada por la Tabla 5.30, se usen los criterios expuestos, a continuación, por la Tabla 5.33 para seleccionar la opción de tratamiento que se ha de aplicar para la mitigación de cada riesgo identificado.

OPCION DE TRATAMIENTO	**CRITERIO**

Retención del riesgo	• Solamente los riesgos pertenecientes a la zona 3 deberían ser retenidos.
	• Se retendrán los riesgos que no pertenezcan a la zona 3 si y solo si:
	  ○ la dirección se compromete a tratar estos riesgos en un futuro cercano.
	  ○ los riesgos no propician el incumplimiento de las derecho del hábeas data o de lo estipulado por la ley de protección de datos personales.

[63] Jefe de la División de Gestión de Investigación

	○ Los riesgos no propician el incumplimiento de alguna obligación contractual. ○ El impacto, sobre la confidencialidad de los activos, causado por el riesgo en particular no es mayor a 5.
Modificación del riesgo	• Los riesgos que no se puedan retener[64] deberían, en lo posible, ser modificados antes que transferidos o evitados.
Transferencia del riesgo	• Si, por restricciones financieras, técnicas, operativas, culturales, éticas, ambientales, legales, de personal o de tiempo, la modificación del riesgo resulta inadecuada, se debería, en lo posible, transferir el riesgo a otra parte que cuente con la capacidad de gestionar de manera más eficaz el riesgo en cuestión. • Solamente los riesgos que pertenezcan a las zonas 1, 2 0 4 serán candidatos para la transferencia de riesgos.
Evitación del riesgo	• La evitación de un riesgo solo será razonable cuando éste pertenezca a la zona 1 o a la zona 4 y después de que se hayan descartado la modificación y la transferencia del riesgo. • A menos de que se justifique, no se debería aplicar la evitación a riesgos que se encuentren en la zona 2.

Tabla 5.33. Criterios para el tratamiento del riesgo

5.3.7. Guía para la valoración de las salvaguardas

De lo discutido por la sección 5.4.1 se puede concluir que la valoración de las salvaguardas es el insumo indispensable para poder estimar los riesgos residuales y por, ende, para poder continuar con la gestión de riesgos de la SI. Lamentablemente, MAGERIT V3 no define ningún criterio para tal fin, solamente afirma, en [22], que las salvaguardas solamente serán consideradas como ideales, o sea 100% eficaces, si y solo sí:

- Están perfectamente definidas, desplegadas, configuradas y mantenidas.
- Son empleadas siempre.
- Son monitoreadas.

Con base en lo anterior, la herramienta PILAR, en el manual [52], define una tabla de criterios que permite valorar las salvaguardas mediante la determinación de su nivel de madurez. Se recomienda usar este aporte y, en lo posible, ajustarlo a las necesidades y particularidades del procedimiento del cual se van a gestionar los

[64] Son aquellos pertenecientes a las zonas 1, 2 o 4

riesgos de SI. Los criterios para la valoración de las salvaguardas que propone PILAR en el manual [52], son expuestos, a continuación por la Tabla 5.34.

Eficacia	**Nivel de madurez**	**Significado** (Según el tipo de salvaguarda del que se trate)
0%	L0	La salvaguarda no existe.
10%	L1	**Procedimiento**: se está empezando a ejecutar o sólo lo ejecutan pocas personas. **Elemento**: se tiene pero apenas se usa **Documento**: se está preparando su elaboración
50%	L2	**Procedimiento**: todos lo hacen igual pero no está documentado. **Elemento**: se tiene pero se está terminando de afinar. **Documento**: se está elaborando.
75%	L3	**Procedimiento**: todos lo hacen igual y está documentado **Elemento**: se tiene y funciona correctamente **Documento**: se tiene
95%	L4	**Procedimiento**: se obtienen indicadores **Elemento**: se obtienen indicadores **Documento**: se obtienen indicadores
100%	L5	**Procedimiento**: es revisado, se proponen mejoras y se aplican **Elemento**: es revisado, se proponen mejoras y se aplican **Documento**: es revisado, se proponen mejoras y se aplican

Tabla 5.34. Criterios para la valoración de las salvaguardas

5.3.8. Técnica para la valoración y tratamiento del riesgo.

En [24] se evidencia que MAGERIT V3 ofrece dos posibles técnicas para la valoración y tratamiento del riesgo: el uso de tablas y el análisis algorítmico. Según [24], el análisis mediante tablas se basa en la distinción y separación de las partes de un todo hasta llegar a conocer sus componentes principales, ignorando los detalles para no alterar la visión de conjunto. El análisis algorítmico, por su parte, permite obtener resultados más precisos y elaborados mediante dos posibles enfoques: cualitativo o cuantitativo.

Los autores de [43], [44] y [45] manifiestan su interés por el enfoque cuantitativo, explicando que por medio de éste se obtienen resultados que, al estar en términos financieros, resultan muy comprensibles. Sin embargo, diferentes obstáculos, como la dificultad para valorar monetariamente activos como la información, hacen necesario que primero se realice un análisis cualitativo, cuyos resultados serán traducidos a cifras financieras mediante métricas para la valoración de los activos, las cuales resultan indispensables cuando se persigue un análisis cuantitativo. Respecto a lo anterior y gracias a [47], se confirma que la herramienta de apoyo PILAR ofrece una tabla de conversión que se encuentra alineada al contexto de las organizaciones españolas y a la legislación vigente para ese país, razón por la cual no resultará adecuada para el caso de estudio.

En Colombia, la Estrategia de Gobierno en Línea [48] ofrece un amplio catálogo de recursos en materia de la SI. Uno de estos es el *CSIRT*[65] *Colombiano* [49] cuya responsabilidad es elaborar y publicar estudios e informes sobre la SI en Colombia con base en estadísticas, indicadores, métricas y otras fuentes. Sin embargo, estos elementos ofrecidos por la Estrategia de Gobierno en Línea no aportan nada relacionado con las métricas para la valoración de activos. Sin este recurso indispensable no será posible conducir un análisis cuantitativo, por lo cual se decide optar por el enfoque cualitativo pues, como se afirma en [46], éste representa la única opción viable cuando los recursos son limitados.

En [22], MAGERIT V3 da otro motivo para descartar el análisis cuantitativo, afirmando que es fácil determinar el precio de elementos tangibles y comerciales como los equipos informáticos, pero que al intentar ponerle precio a activos más abstractos e intangibles, como la información, la valoración cuantitativa puede ser escurridiza y motivo de agrias disputas entre expertos, entorpeciendo la gestión de riesgos de la SI.

Por todo lo anterior, para la gestión de riesgos de la SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca, se recomienda conducir un análisis cualitativo en lugar de un cuantitativo.

[65] Por sus siglas en inglés: Computer Security Incident Response Team, que traduce: *Equipo de respuesta a incidentes de la seguridad computacional.*

5.4. Confrontación entre MAGERIT V3 y la adaptación propuesta

Con el fin de aclarar la magnitud de los aportes hechos por esta adaptación de la metodología MAGERIT V3, a continuación, la Tabla 5.1 expone una comparación entre la versión original y la versión adaptada.

ASPECTO A EVALUAR	VERSIÓN ORIGINAL	VERSIÓN ADAPTADA
Provee un esquema para la clasificación de la información que contemple el contexto del caso de estudio.	NO	SI
Define una organización, para operar la gestión de riesgos de la SI, que considere la estructura funcional de la Universidad del Cauca.	NO	SI
Define criterios para la valoración de activos.	PARCIAL	SI
Define criterios para la valoración de amenazas.	NO	SI
Define criterios para la evaluación del riesgo.	NO	SI
Define criterios para el tratamiento del riesgo.	NO	SI
Define criterios para valorar las salvaguardas.	NO	SI
Cumple los requerimientos de la norma ISO/IEC 27001 [2], al garantizar que las salvaguardas (controles) se seleccionarán solamente después de haber estimado y priorizado los riesgos	NO	SI

Tabla 5.35. Confrontación entre MAGERIT V3 y la adaptación propuesta

Capitulo 6

Validación de la solución

Durante esta cuarta etapa del desarrollo del proyecto se ejercita la solución y se corrigen los errores detectados. De acuerdo con lo anterior, se usa el MARA, producto de las adaptaciones hechas a la metodología MAGERIT V3, para ejecutar la fase 4 del proceso de planeación de un SGSI: V*aloración del riesgo y planeación del tratamiento del riesgo*[66].

Los resultados, obtenidos de usar el MARA para ejecutar la fase 4 del proceso de planeación de un SGSI, son expuestos por la sección 6.1. Por recomendaciones de [68]: un estudio observacional conducido sobre una empresa de desarrollo de Software, los resultados serán representados por diagramas de tartas, también conocidos como gráficos circulares. De esta manera se logra satisfacer el entregable: *Reportes de la valoración del riesgo,* requerido por la fase 4 del proceso de planeación de un SGSI.

A medida que se ejercita la adaptación se logra evaluar su desempeño como mecanismo para la gestión de riesgos, permitiendo identificar algunos defectos en su formulación, los cuales son expuestas por la sección 6.2. Luego, con base en las fallas identificadas por la sección 6.2, se realizan los respectivos ajustes a la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3 como mecanismo para la gestión de riesgos de la SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca.

Finalmente, cabe mencionar que los autores de [64] proponen el uso de las encuestas como solución a la poca validación empírica de los estudios relacionados con las ciencias de la computación. En razón de lo expuesto y para terminar de validar la adaptación propuesta, fue necesario realizar una serie de encuestas para someter a la adaptación a la evaluación por parte de expertos y por parte del usuario de la misma.

---

[66] Ver la Figura 2.2

6.1. Ejercitación de la solución

A continuación, las secciones 6.1.1, 6.1.2, 6.1.3 y 6.1.4 exponen los resultados de ejecutar cada una de las tareas formuladas por el MARA que, de acuerdo con el mapeo ilustrado por la Tabla 6.1, lograron satisfacer todas las actividades y entregables definidos por la fase 4 del proceso de planeación de un SGSI.

TAREAS DEFINIDAS POR EL MARA	ACTIVIDADES DEFINIDAS POR LA FASE 4 DEL PROCESO DE PLANEACION DE UN SGSI
MARA.1. Caracterización de los activos. MARA.2. Caracterización de las amenazas. MARA.3. Estimación del estado del riesgo.	• Valorar el riesgo
MARA.4. Caracterización de las salvaguardas	• Seleccionar los objetivos de control y los controles. • Obtener aprobación para implementar y operar el SGSI.

Tabla 6.1. Mapeo de actividades

6.1.1. MARA.1. Caracterización de activos.

❖ **MARA.1.1. Definir un esquema para la clasificación de la información**

Atendiendo las orientaciones suministradas por la sección 5.3.1, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se resuelve usar el esquema expuesto para llevar a cabo la clasificación de la información vinculada al caso de estudio.

❖ **MARA.1.2. Definir la organización para la gestión del riesgo.**

Atendiendo las orientaciones suministradas por la sección 5.3.2, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se resuelve usar la organización de roles y responsabilidades expuesta por la Tabla 3.1.

❖ **MARA.1.3. Definir los criterios para la valoración de activos.**

Atendiendo las orientaciones suministradas por la sección 5.3.3, de la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3, se resuelve usar los criterios expuestos por la Tabla 5.22.

- **MARA.1.4. Identificación de los activos.**
  Esta actividad considera como elementos de entrada:

- El documento [32] mediante el cual se especifica el caso de estudio.
- La caracterización funcional de los puestos de trabajo, expuesta en [91].
- Los locales y sedes de la Universidad identificadas por la sección 4.1.2.
- El esquema para la clasificación de la información expuesto por la Tabla 5.19

Con base en lo anterior, se obtiene el inventario de activos expuesto por la sección 4.3.2 en la Tabla 4.1, logrando satisfacer el producto de salida: *Relación de activos a considerar,* especificado por la presente tarea. Asimismo, se abona los entregables "*Activos identificados"* y "*Clasificación de activos",* los cuales son requeridos por la fase 3 del proceso de planeación de un SGSI, ilustrado por la Figura 2.2.

- **MARA.1.5. Identificación de dependencias.**

A la hora de identificar y diagramar las dependencias entre los activos, PILAR puede resultar de gran ayuda, no obstante, el uso de esta herramienta requiere que los activos sean agrupados por "*capas",* las cuales no tienen ningún impacto en la valoración de riesgos, pues no son más que una manera de organizar los activos para una mejor comprensión y comunicación. En virtud de lo señalado, fue necesario agrupar los activos por capas como lo muestra, a continuación, la Tabla 6.2.

CAPA	ACTIVOS CUBIERTOS
Activos esenciales	Activos de tipo información y de tipo servicios
Sistemas de información	SIVRI
Soportes de información	Documentos físicos Dispositivos de almacenamiento de información digital.
Equipos informáticos	Servidores Computadores personales Fotocopiadoras multifuncionales Reloj radicador
Redes	Redes de área local (LAN y WLAN)
Personal	Personal
Equipos auxiliares	Satélite (sistema de archivo), Equipos de climatización y UPS
Instalaciones	Oficinas del personal, Cuarto de servidores y Almacenes Archivo Satélite VRI

Tabla 6.2. Organización de los activos por capas

Considerando las capas definidas anteriormente, el documento [32] mediante el cual se especifica el caso de estudio los productos de salida de la anterior tarea, el producto

de la tarea anterior: *Relación de activos a considerar* y las indicaciones del jefe de la División de Gestión de la Investigación[67], se logra obtener, con la ayuda de PILAR, el diagrama de las dependencias que existen entre los activos de información, el cual es ilustrado, a continuación, por la Figura 6.1.

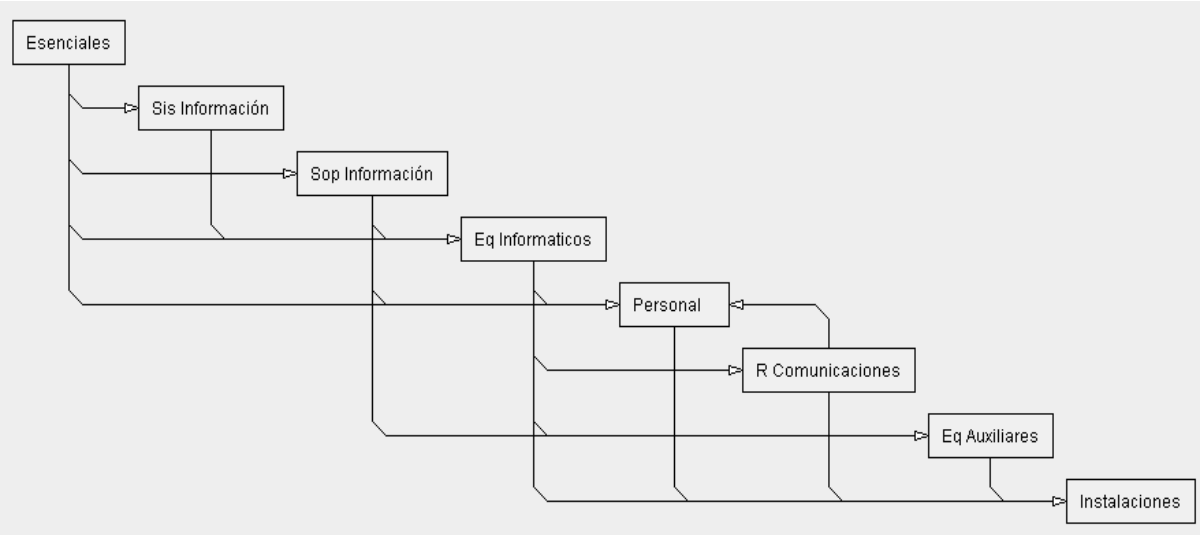

Figura 6.1. Diagrama de dependencias entre activos. Fuente: PILAR

En el Anexo C.1.1 se expone una tabla que describe, en detalle, las dependencias que existen entre los activos de información vinculados al caso de estudio. Por todo lo anterior, se logra satisfacer el único producto de salida requerido por esta tarea.

- **MARA.1.6. Valoración de los activos**

Al intentar valorar los activos vinculados al caso de estudio se encontró que, en [22], MAGERIT V3 propone valorar 5 dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, no obstante, las únicas dimensiones que la norma ISO/IEC 27001 [2] exige tener en cuenta son la confidencialidad, integridad y la disponibilidad. Además, en [22] MAGERIT V3 manifiesta que la autenticidad y la trazabilidad fueron añadidas como dimensiones complementarias encaminadas a mantener la integridad y la confidencialidad.

En razón de lo expuesto, se consideró pertinente valorar solamente las 3 dimensiones primarias: confidencialidad, integridad y disponibilidad, para lo cual se acudió a los criterios expuestos por la Tabla 5.22. Para poder hacer uso de PILAR y facilitar la valoración de los activos, fue necesario cargar esta herramienta con los criterios expuestos por la Tabla 5.22 siguiendo las instrucciones suministradas por el Anexo A.3.2.

[67] Responsable de la ejecución del caso de estudio.

Luego, para valorar las dimensiones primarias de cada activo con la ayuda de PILAR y los criterios propuestos por la sección 5.3.3, resultó necesario preguntarse:

- En cuanto a la confidencialidad: ¿qué daño causaría que el activo sea conocido por quien no debe? ¿Qué consecuencias traería la divulgación de información que no sea pública? Luego de pensar en las posibles consecuencias, se deberá seleccionar, en PILAR, los criterios que se cumplen si la confidencialidad del activo se ve comprometida. PILAR calculará el valor de esta dimensión como el mayor valor de los criterios seleccionados.

- En cuanto a la integridad: ¿qué perjuicio causaría que el activo estuviera dañado o corrupto? Esta valoración es típica de los datos que pueden estar manipulados, ser total o parcialmente falsos o, incluso, estar incompletos. Luego de pensar en las posibles consecuencias, se deberá seleccionar, en PILAR, los criterios que se cumplen si la integridad del activo se ve comprometida. PILAR calculará el valor de esta dimensión como el mayor valor de los criterios seleccionados.

- En cuanto a la disponibilidad: ¿qué perjuicio causaría no tener el activo o no poder utilizarlo? Luego de pensar en las posibles consecuencias, se deberá seleccionar, en PILAR, los criterios que se cumplen si la disponibilidad del activo se ve comprometida. PILAR calculará el valor de esta dimensión como el mayor valor de los criterios seleccionados.

Por otra parte, se logró identificar que MAGERIT V3 manifiesta que el valor nuclear suele estar en los activos esenciales que, como se mencionó anteriormente, corresponden a la información gestionada y los servicios que se prestan, quedando los demás activos subordinados a las necesidades de protección de lo esencial. Según MAGERIT V3, todo activo que no sea de tipo información o servicios no necesitará que se le asigne valor propio, pues éstos resultan valiosos en la medida en que soporten los activos esenciales.

En virtud de lo señalado, se consideró conveniente valorar únicamente los activos esenciales y dejar que el valor de los demás activos se determine como el acumulado de los valores que éstos heredan de sus superiores a través de las dependencias.

Con el apoyo de PILAR, ya cargada con los criterios expuestos por la Tabla 5.22 y considerando lo discutido anteriormente, los criterios para la valoración de activos definidos por la tarea MARA.1.3, los productos de las tareas previas y la guía suministrada por la sección 5.3.3, se logró valorar las 3 dimensiones primarias de los activos esenciales en compañía del responsable del caso de estudio: el Jefe de la División de Gestión de Investigación. A modo de evidencia, en [92] se encuentran disponibles las grabaciones de audio de la entrevista realizada.

Luego, el valor se propagó, por medio de las dependencias, hacia los activos no esenciales, obteniendo, con ayuda de PILAR, los resultados expuestos por el Anexo C.1.2, de los cuales se puede concluir que:

- Observando la dimensión de la confidencialidad:
  - El 69% de los activos tienen un valor muy alto en esta dimensión
  - El 16% de los activos tienen un valor alto en esta dimensión
  - Ningún activo tiene un valor medio para su confidencialidad.
  - El 3% de los activos tienen un bajo en esta dimensión
  - El 12% de los activos tienen un valor despreciable en esta dimensión

- Observando la dimensión de la disponibilidad.
  - El 63% de los activos tienen un valor muy alto en esta dimensión
  - El 34% de los activos tienen un valor alto en esta dimensión
  - El 3% de los activos tienen un valor medio en esta dimensión
  - Ningún activo tiene un valor bajo para su disponibilidad.
  - Ningún activo tiene un valor despreciable para su disponibilidad.

- Observando la dimensión de la integridad.
  - El 69% de los activos tienen un valor muy alto en esta dimensión
  - El 15% de los activos tienen un valor alto en esta dimensión
  - Ningún activo tiene un valor medio para su integridad.
  - Ningún activo tiene un valor bajo para su integridad.
  - El 16% de los activos tienen un valor despreciable en esta dimensión

Estas proporciones son ilustradas, a continuación, por las Figuras 6.2, 6.3 y 6.4 respectivamente. Cabe mencionar que de los 39 activos identificados inicialmente, siete fueron excluidos de la gestión de riesgos de la SI porque su valor promedio estaba en el nivel despreciable, de acuerdo con la escala para la valoración de los activos expuesta por la Tabla 5.21.

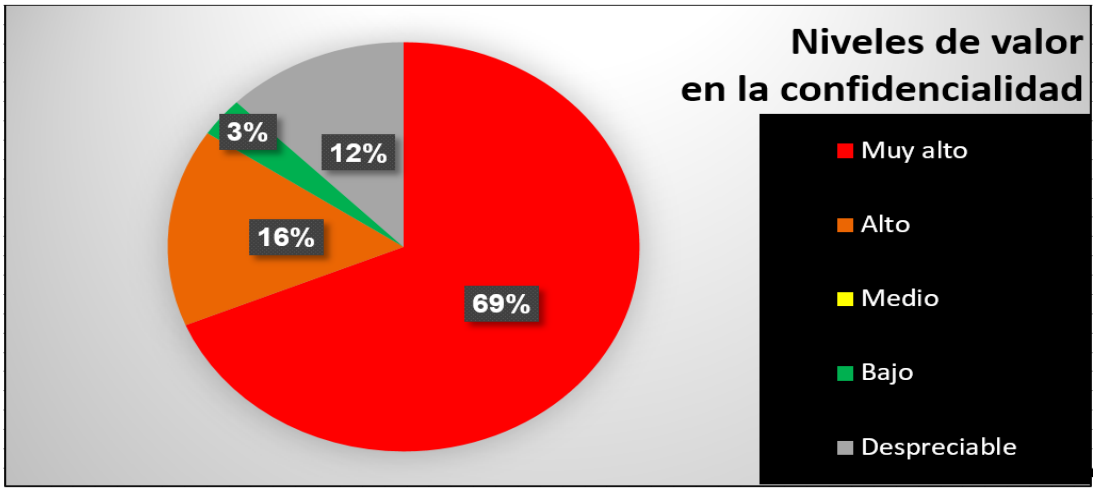

Figura 6.2. Los activos y su nivel de valor en la confidencialidad

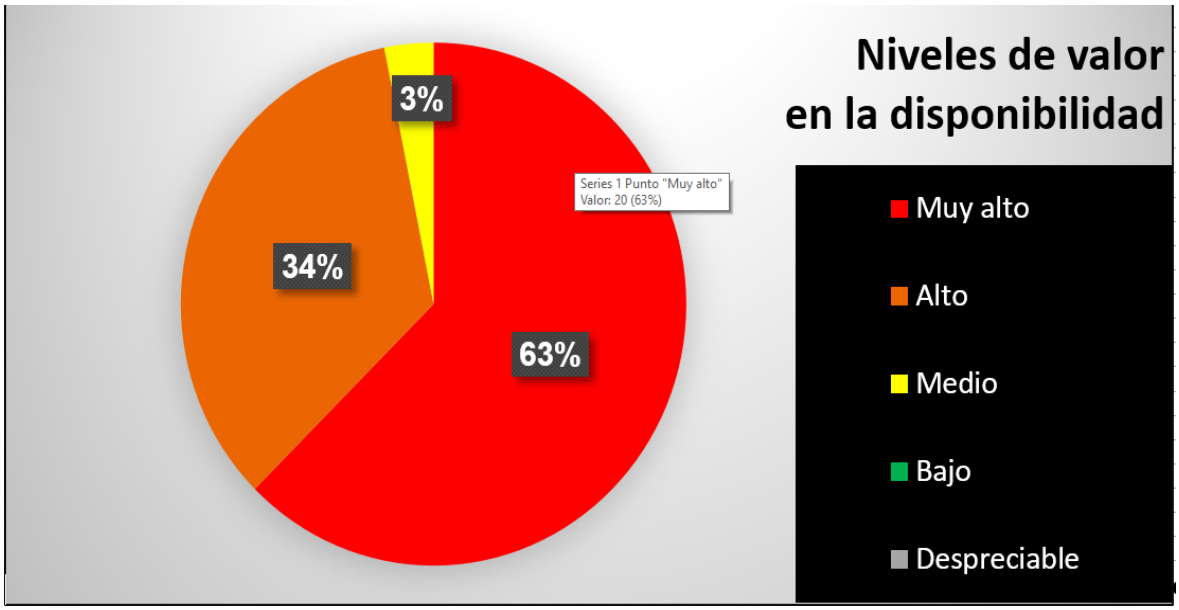

Figura 6.3. Los activos y su nivel de valor en la disponibilidad

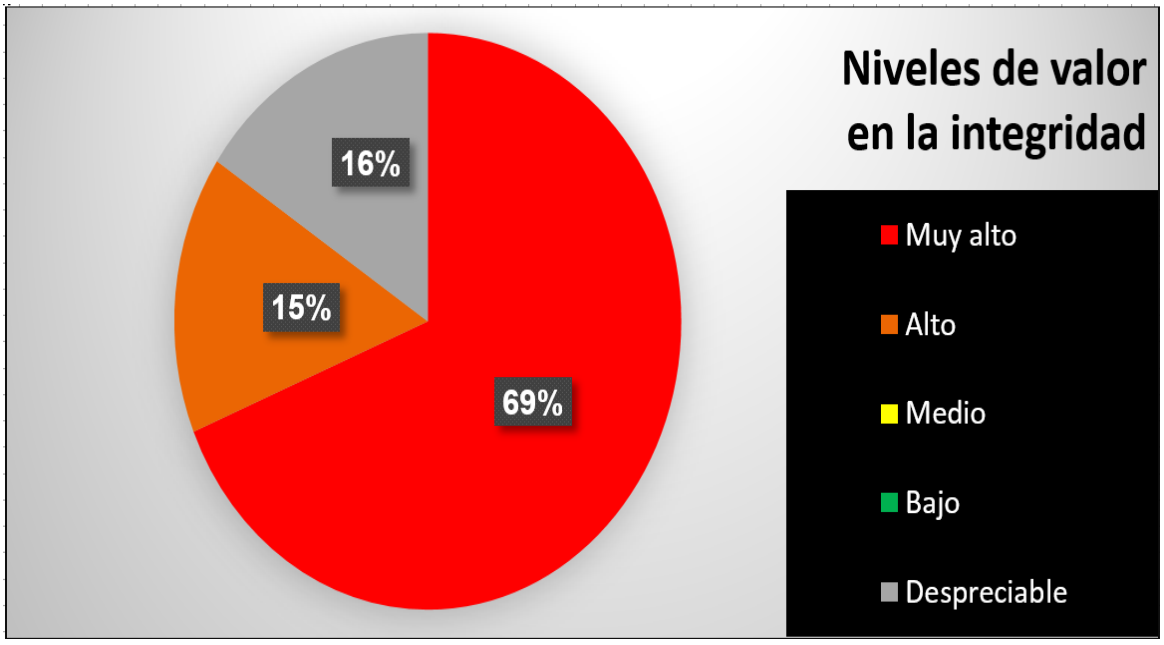

Figura 6.4. Los activos y su nivel de valor en la integridad

Gracias a todo lo anterior, se logra satisfacer el producto de salida: *Modelo de valor,* requerido por la presente tarea.

6.1.2. MARA.2. Caracterización de las amenazas

- **MARA.2.1. Definir los criterios para la valoración de amenazas.**

Atendiendo la guía suministrada por la sección 5.2.1, se resuelve usar los criterios para la valoración de amenazas expuestos por la sección 5.3.4.

- **MARA.2.2. Identificación de las amenazas**

Al intentar ejecutar esta actividad, se encontró que en [22], MAGERIT V3 afirma que las amenazas no suelen materializarse sobre los activos esenciales sino, más bien, en los activos que los soportan, propagando su degradación a través de las dependencias existentes. En razón de lo expuesto, se consideró totalmente innecesario intentar identificar amenazas sobre los activos esenciales.

Considerando lo discutido anteriormente, la guía suministrada por la sección 5.3.4, los productos de salida de las tareas previas, el informe de vulnerabilidades expuesto por la sección 4.3.3 y el catálogo de amenazas ofrecido por PILAR, se lograron identificar las amenazas que atentan contra los activos vinculados al caso de estudio. Los resultados son expuestos por el Anexo C.2 en la Tabla C.4, logrando, de ese modo, satisfacer el producto de salida: *Relación de amenazas posibles,* requerido por la presente tarea.

- **MARA.2.3.Valoración de las amenazas**

Al intentar ejecutar esta actividad, se encontró que determinar la probabilidad de ocurrencia de las amenazas y la degradación causada sobre cada activo, en cada dimensión, es una tarea desmoralizadora según MAGERIT V3[68], por lo cual sugiere partir de datos estándar que sean ajustados hasta reflejar, con la mayor precisión posible, la realidad del caso de estudio. Por la amplia trayectoria, uso y reconocimiento de PILAR, se decidió valorar las amenazas tomando, como punto de partida, los datos estándar de la biblioteca que provee ésta herramienta.

Los criterios propuestos en la sección 5.3.4 fueron de gran ayuda para ajustar los valores de las amenazas, suministrados por PILAR, a las particularidades del contexto del caso de estudio como el nivel de conciencia y conocimiento en materia de la SI por parte del personal, a las condiciones climáticas de Popayán[69] y a las frecuentes interrupciones del suministro de energía a causa de las tormentas eléctricas, etc. De igual manera, resultaron útiles para valorar amenazas desconocidas por la biblioteca de datos de PILAR.

Considerando lo discutido anteriormente, la guía suministrada por la sección 5.3.4, las escalas y criterios definidos por la sección 5.3.4, informe de vulnerabilidades expuesto por la sección 4.3.3 y el producto de salida de la tarea anterior: *Relación de amenazas*

[68] Ver la sección 8.6 del documento [22]

[69] Por ejemplo, en la ciudad de Popayán se puede presentar una mayor probabilidad de que se materialicen amenazas como las inundaciones.

posibles, se logró determinar, con ayuda de PILAR, la probabilidad de ocurrencia de las amenazas y la degradación que éstas causan sobre el valor de los activos. Los resultados son expuestos por el Anexo C.2 en la Tabla C.4, de los cuales se puede concluir que:

- En cuanto a la probabilidad de ocurrencia:
    - El 9% de las amenazas seguramente se materializarán.
    - La ocurrencia del 38% de las amenazas es altamente probable.
    - El 31% de las amenazas posiblemente se materializarán.
    - El 11% de las amenazas son poco probables.
    - El 11% de las amenazas raramente se materializaran.

- En cuanto a la degradación que causan las amenazas sobre la confidencialidad de los activos:
    - El 17% de las amenazas causan una degradación muy alta.
    - El 15% de las amenazas causan una degradación media
    - El 12% de las amenazas causan una degradación baja
    - El 56% de las amenazas causan una degradación despreciable

- En cuanto a la degradación que causan las amenazas sobre la disponibilidad de los activos:
    - El 30% de las amenazas causan una degradación muy alta.
    - El 1% de las amenazas causan una degradación alta.
    - El 21% de las amenazas causan una degradación media
    - El 17% de las amenazas causan una degradación baja
    - El 31% de las amenazas causan una degradación despreciable

- En cuanto a la degradación que causan las amenazas sobre la integridad de los activos:
    - El 12% de las amenazas causan una degradación muy alta.
    - El 7% de las amenazas causan una degradación media
    - El 19% de las amenazas causan una degradación baja
    - El 62% de las amenazas causan una degradación despreciable

Estas proporciones son ilustradas, a continuación, por las Figuras 6.5, 6.6, 6.7 y 6.8

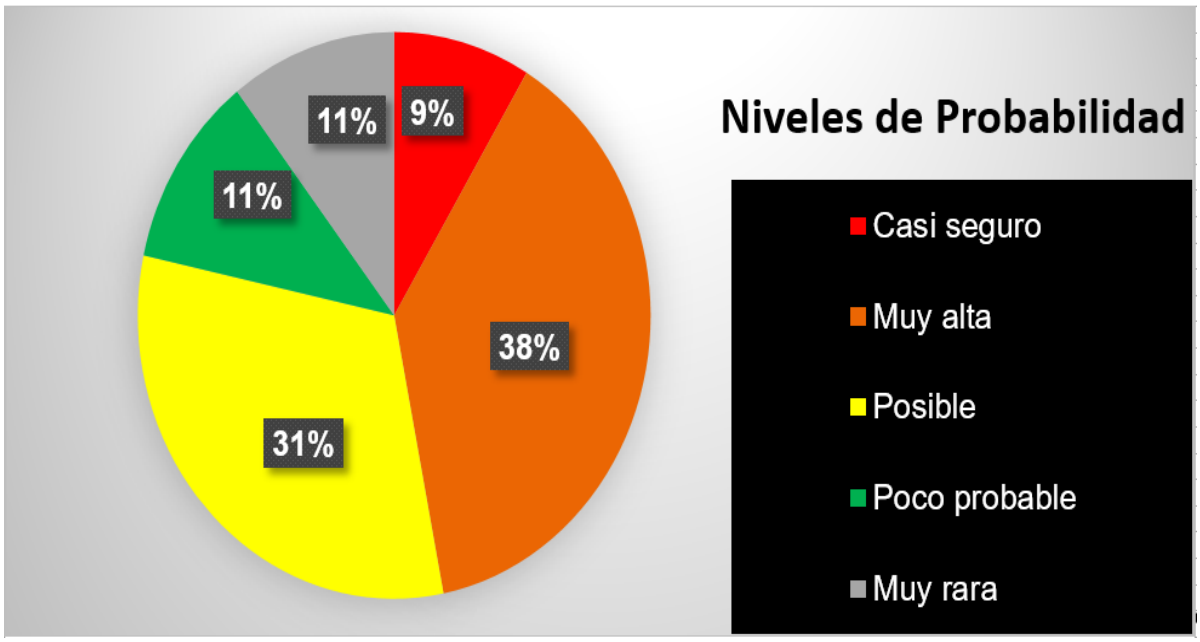

Figura 6.5. Las amenazas y su nivel de probabilidad de ocurrencia

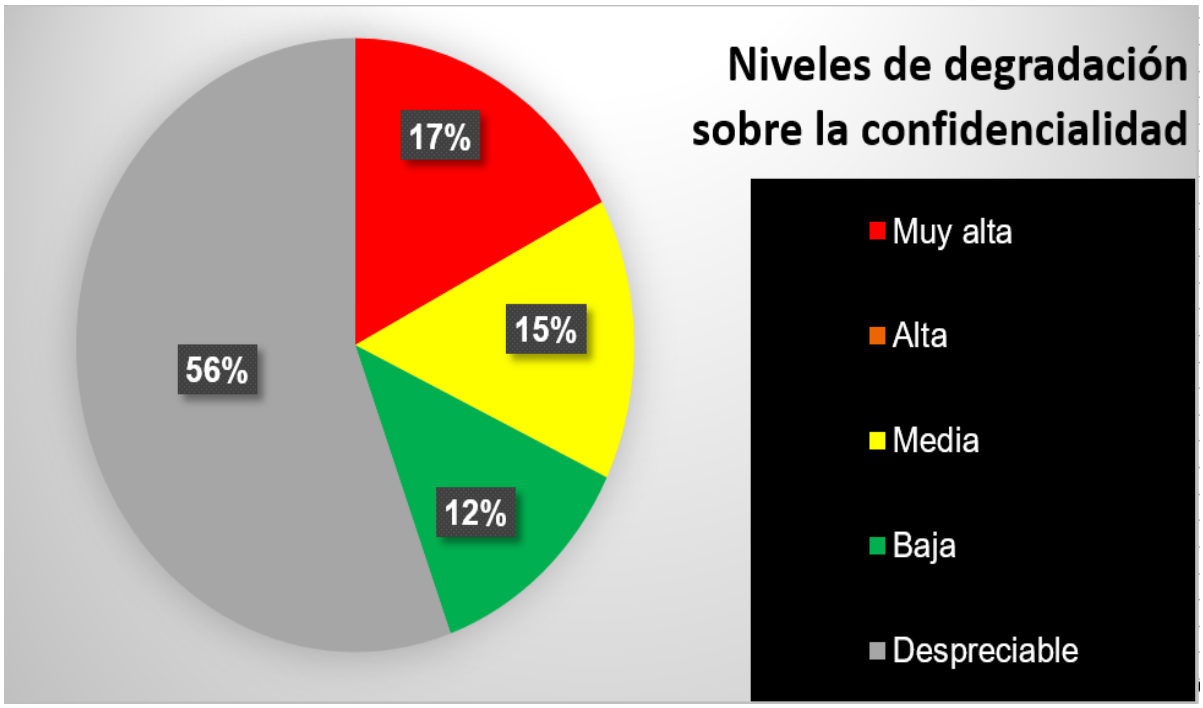

Figura 6.6. Las amenazas y el nivel de degradación que pueden causar sobre la confidencialidad de los activos

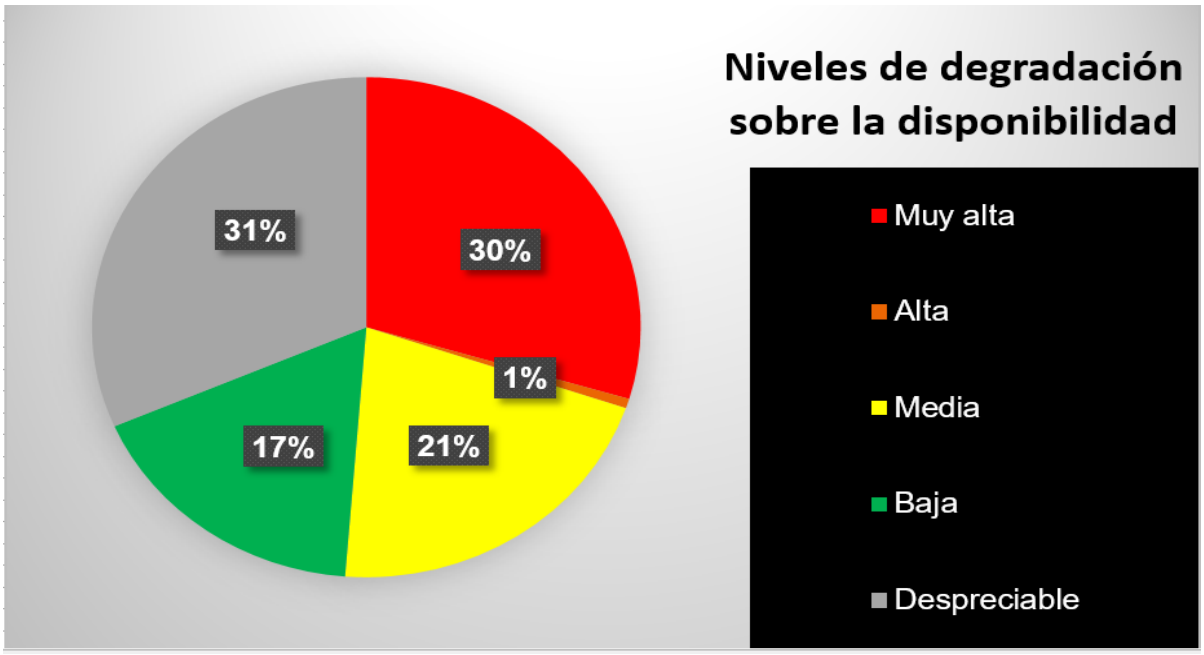

Figura 6.7. Las amenazas y el nivel de degradación que pueden causar sobre la disponibilidad de los activos

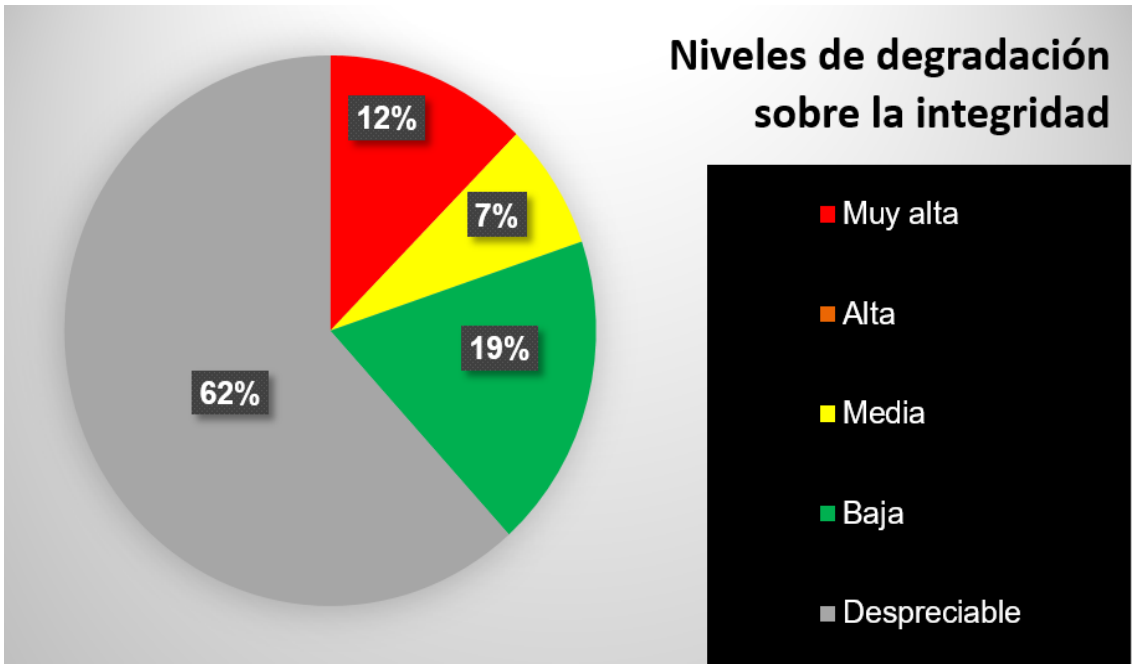

Figura 6.8. Las amenazas y el nivel de degradación que pueden causar sobre la integridad de los activos

Gracias a todo lo anterior, se logra satisfacer el producto de salida: *Mapa de riesgos,* requerido por la presente tarea. Cabe mencionar que la presente actividad definía la entrada: Histórico de incidentes, no obstante, en la VRI no se conserva ningún registro de eventos que permitiera satisfacer este producto de entrada.

6.1.3. MARA.3. Estimación del estado del riesgo

- **MARA.3.1. Definir criterios para la evaluación del riesgo**

Atendiendo la guía suministrada por la sección 5.3.1, se resuelve usar los criterios para la evaluación del riesgo expuestos por la sección 5.3.5.

- **MARA.3.2. Estimación del impacto**

En la sección 4.3 se identificó que el personal posee un nivel de conciencia y conocimiento, en cuestiones de la SI, que no va más allá de la implementación de controles sencillos como la instalación de antivirus, el uso contraseñas para el inicio de sesión en las estaciones de trabajo y el uso de archivadores para almacenar los documentos bajo llave.

Consecuentemente, no se han diseñado ni implementado formalmente los controles para proteger los activos de información vinculados al caso de estudio. De este modo, se evidencia una desatención generalizada por la SI y un desconocimiento total de los controles que la norma ISO/IEC 27001 [2] sugiere en su Anexo A.

Considerando lo discutido anteriormente y los productos de las tareas previas MARA.1. *Caracterización de los activos* y MARA.2. *Caracterización de las amenazas*, se logró, con ayuda de PILAR, estimar el impacto potencial al que se encuentran sometidos los activos de información vinculados al caso de estudio. Los resultados son expuestos por el Anexo C.3 en la Tabla C.5, logrando, de ese modo, satisfacer el producto de salida: *Informe de impacto potencial,* requerido por la presente tarea.

- **MARA.3.3. Estimación del riesgo**

Con base en el *Informe de impacto potencial,* obtenido de la tarea MARA.3.2, y el *Mapa de Riesgos* obtenido de la tarea MARA.2.3, la herramienta PILAR logró calcular y estimar los riesgos, para cada dimensión primaria. Luego, teniendo en cuenta las directrices definidas por la sección 5.3.5 para el cálculo del valor ponderado del riesgo y la escala ilustrada por la Tabla 5.30, se obtuvo que, de los 162 riesgos estimados por PILAR:

- El 4% son críticos
- El 6% son riesgos de alta magnitud.
- El 20% son riesgos medios.
- El 22% son riesgos de baja magnitud.

- El 48% son despreciables. De acuerdo con los criterios propuestos por la sección 5.3.5 en la Tabla 5.32, estos riesgos serán excluidos del tratamiento y, por ende, no serán tenidos en cuenta durante la selección de salvaguardas.

Estas proporciones son ilustradas, a continuación, por la Figura 6.9.

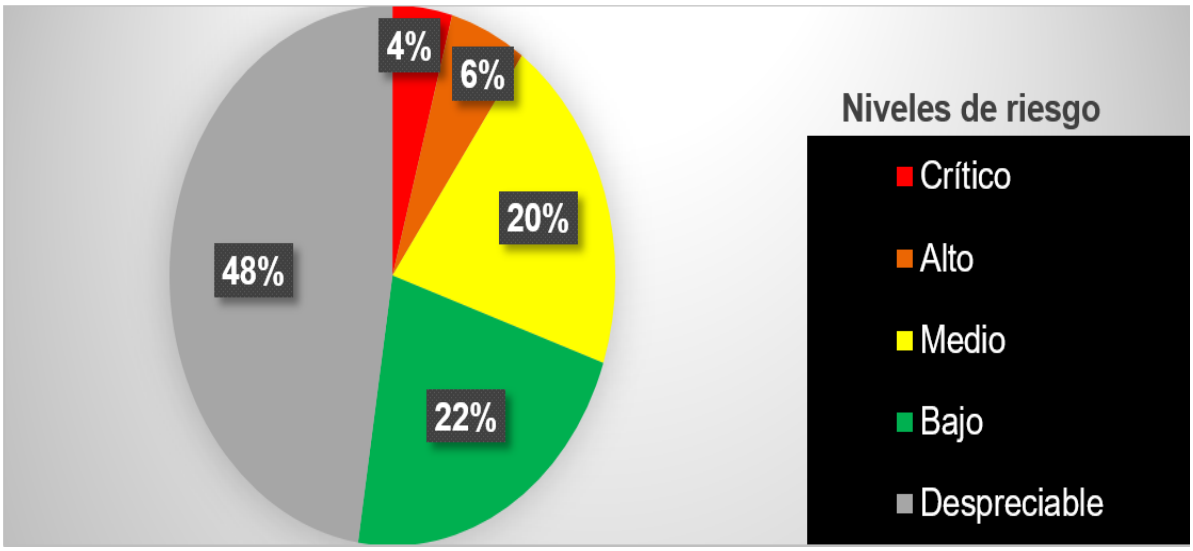

Figura 6.9. Riesgos sobre los activos no esenciales

Luego, dando cumplimiento a la cláusula 6.1.2.e) de la norma ISO/IEC 27001 [2], se procede a priorizar los riesgos mediante la aplicación de los criterios para la evaluación del riesgo, propuestos por la sección 5.3.5 en la Tabla 5.32. Los resultados son expuestos por el Anexo C.3 en la Tabla C.5[70].

Cabe mencionar que los riesgos, identificados anteriormente, se propagaron hacia los activos esenciales a través de las dependencias. Gracias al apoyo de la herramienta PILAR, fue posible determinar el nivel de riesgo al que se encontraban sometidos los activos esenciales como consecuencia de dicha propagación. Los resultados son expuestos por el Anexo C.3 en la Tabla C.6, de lo cual se puede concluir que:

- El 56% de los activos esenciales se expone a un nivel de riesgo crítico.
- El 28% de los activos esenciales se expone a un nivel de riesgo alto.
- El 5% de los activos esenciales se expone a un nivel de riesgo medio.
- El 11% de los activos esenciales se expone a un nivel de riesgo bajo.
- No hay activo esencial que se exponga a riesgos despreciables.

Estas proporciones son ilustradas, a continuación, por la Figura 6.10.

[70] Se aclara que, de acuerdo con los criterios propuestos por la sección 5.3.5 en la Tabla 5.33, los riesgos con un valor ponderado *Despreciable,* serán excluidos de la Tabla C.5.

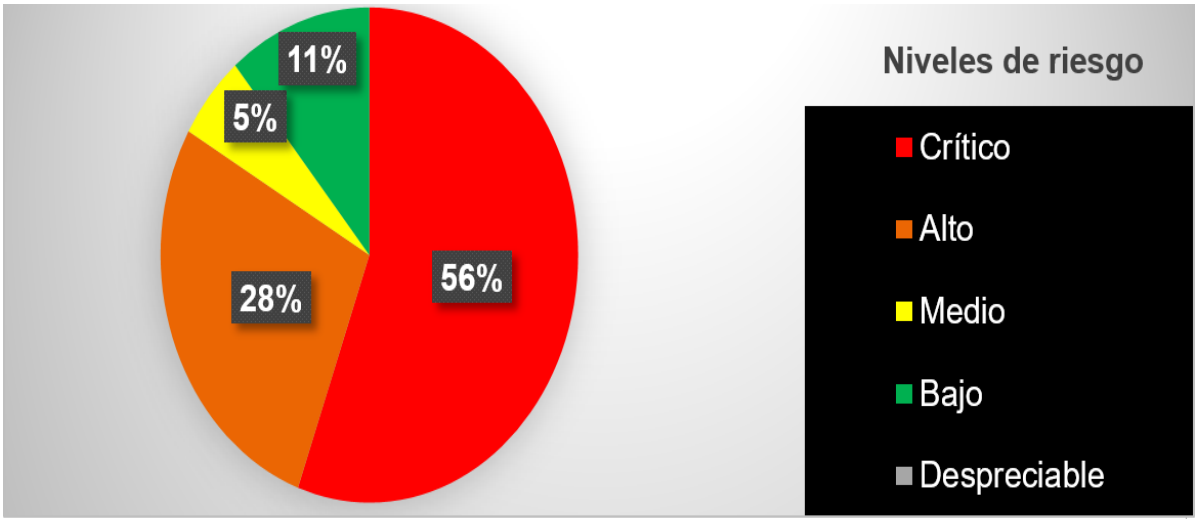

Figura 6.10. Porcentaje de activos esenciales expuestos a cada nivel de riesgo

Por todo lo anterior, se logra satisfacer el producto de salida: *informe de riesgo potencial,* requerido por la presente tarea.

6.1.4. MARA.4. Caracterización de las salvaguardas

- **MARA.4.1. Definir criterios para la valoración de las salvaguardas**

Atendiendo la guía suministrada por la sección 5.4.1, se resuelve usar los criterios para la evaluación de salvaguardas expuestos por la sección 5.3.7.

- **MARA.4.2. Definir criterios para el tratamiento del riesgo**

Atendiendo la guía suministrada por la sección 5.4.2, se resuelve usar los criterios para el tratamiento del riesgo expuestos por la sección 5.3.6.

- **MARA.4.3. Identificación de las salvaguardas**

Frente a las cuatro opciones de tratamiento disponibles, y descritas por la Tabla 2.1, resultó necesario acudir a los criterios definidos por la sección 5.3.6 en la Tabla 5.33, a fin de tomar decisiones reproducibles, objetivas e imparciales que permitieran elegir la opción de tratamiento más adecuada para mitigar cada uno de los 85 riesgos prioritarios[71] que fueron identificados por el *Informe de riesgo potencial,* obtenido de la tarea MARA.3.3.

[71] Cabe recordar que, como se mencionó en la sección 6.3.3, el 48% de los riesgos presentaron un valor despreciable. De acuerdo con los criterios propuestos por la sección 5.3.5 en la Tabla 5.33, estos riesgos debieron ser excluidos del tratamiento, lo cual explica la razón por la cual la selección de salvaguardas (controles) sólo consideró 85 de los 162 riesgos identificados inicialmente.

De acuerdo con la guía suministrada por la sección 5.4.3, para los riesgos que tuvieron que ser tratados con la opción: *Modificación*[72]*,* se tomó como referente los controles ofrecidos por el Anexo A de la norma ISO/IEC 27001 [2], de los cuales se seleccionaron, únicamente, los que fueron necesarios para mitigar cada riesgo.

Como resultado de la selección de las salvaguardas se obtuvo el *Plan de Tratamiento de Riesgos (PTR)*, el cual es expuesto, en detalle, en el Anexo C.4.1, logrando satisfacer los entregables: *Plan del tratamiento del Riesgo* y la *Lista de controles y objetivos de control seleccionados*, requeridos por la presente tarea y por la fase 4 del proceso de planeación de un SGSI[73]. A partir del PTR se puede concluir que:

- El 21% de los riesgos serán *retenidos* (o aceptados).
- El 71% de los riesgos serán modificados mediante la implementación de controles.
- El 6% de los riesgos serán transferidos a otra parte que los pueda gestionar de manera más eficaz.
- El 2% de los riesgos serán evitados pues, según el estándar ISO/IEC 27005 [5], evitar los riesgos causados por la naturaleza puede ser una alternativa más eficaz.

Estas proporciones son ilustradas, a continuación, por la Figura 6.11.

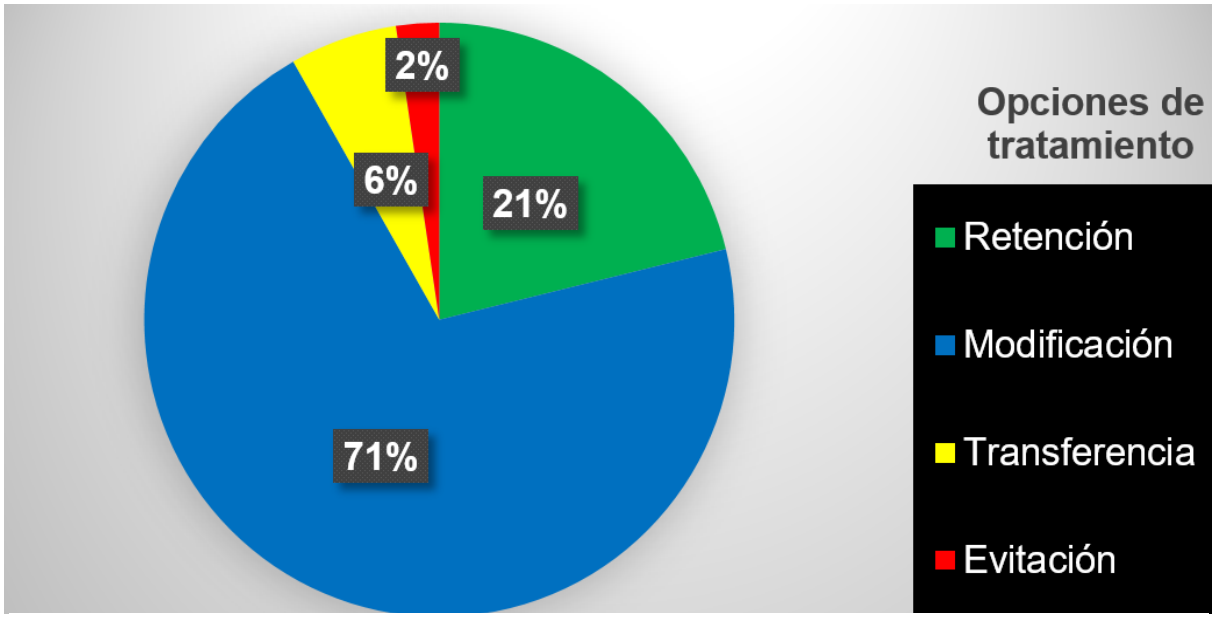

Figura 6.11. Porcentaje de activos esenciales expuestos a cada nivel de riesgo

[72] Como lo expone la Tabla 2.1, la opción de tratamiento: *Modificación,* implica la selección e implementación de controles.
[73] Ilustrado por la Figura 2.2

❖ **MARA.4.4. Valoración de las salvaguardas**

De acuerdo con los criterios para la valoración de salvaguardas, propuestos por la sección 5.3.7 en la Tabla 5.34, la herramienta PILAR calculó que las salvaguardas (controles) deberán alcanzar un grado de madurez L3 para lograr mitigar los riesgos hasta el nivel aceptable propuesto en la sección 5.3.6[74]. PILAR estima que, cuando se den estas condiciones, todos los riesgos residuales, a los cual se exponen los activos de información, serán reducidos a niveles despreciables.

Los resultados de la estimación del riesgo residual son expuestos, en detalle, por [55], logrando satisfacer el producto de salida: *Informe de riesgo residual,* requerido por la presente tarea.

❖ **MARA.4.5. Aceptación de riesgos**

Como lo evidencia el *Informe de riesgo residual* [55], todos los riesgos fueron reducidos al nivel *Despreciable,* de acuerdo con la escala propuesta por la Tabla 5.30, lo cual hizo posible que la Dirección aceptara todos los riesgos residuales y aprobara el PTR. Esta decisión es comunicada, de manera escrita, por el jefe de la División de Gestión de Investigación, quien tiene a su cargo la responsabilidad del caso de estudio. Dicho comunicado es expuesto, a manera de evidencia, por el Anexo C.4.2. De esta manera se logra satisfacer los siguientes entregables, requeridos por la presente tarea y por la fase 4 del proceso de planeación de un SGSI:

- *Aceptación de riesgos residuales*.
- *Aprobación del Plan de Tratamiento de Riesgos (PTR)*

El estándar ISO/IEC 27003 [4] establece que, una vez se hayan aceptado todos los riesgos, se deberá preparar la Declaración de Aplicabilidad (SOA) con el fin de esclarecer cuáles de los 144 controles sugeridos por el Anexo A de la norma ISO/IEC 27001 [2] deberán ser implementados en el caso de estudio para mitigar, adecuadamente, los riesgos de la SI previamente identificados. En la SOA se deberá justificar claramente cualquier inclusión y exclusión de los controles listados por el Anexo A.

La SOA obtenida del tratamiento de riesgos de la SI en el caso de estudio, se expone en el Anexo C.4.3, logrando satisfacer, de esa manera, el entregable: *Declaración de Aplicabilidad (SOA),* requerido por la presente tarea y por la fase 4 del proceso de planeación de un SGSI.

[74] El nivel de riesgo aceptable es *Bajo,* considerando la escala ilustrada por la Tabla 5.30.

6.2. Evaluación y ajuste de la solución

En la presente sección se exponen los resultados de las actividades encaminadas a evaluar el desempeño de la adaptación propuesta como mecanismo para la gestión de riesgos de la SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca.

6.2.1. Fallas identificadas en la adaptación

- **Fallas en la valoración de los activos**

En la sección 6.1.1, mientras se valoraban los activos de información vinculados al caso de estudio, se identificó que la adaptación no consideró las dimensiones que deberían ser valoradas para gestionar adecuadamente los riesgos de la SI. Consecuentemente, no hubo otra opción más que consultar los lineamientos proporcionados por MAGERIT V3 que, en [22], propone valorar 5 dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

De esta manera, la adaptación propuesta ignoraba por completo que las únicas dimensiones que la norma ISO/IEC 27001 [2] exige tener en cuenta son la confidencialidad, integridad y la disponibilidad. Además, se desconocía que, en [22], MAGERIT V3 declara que la autenticidad y la trazabilidad fueron añadidas como dimensiones complementarias encaminadas a mantener la integridad y la confidencialidad.

Por otra parte, cuando se formuló la adaptación, se desconocía que, según MAGERIT V3, el valor nuclear se concentra en los activos esenciales y que, por ende, todo activo que no sea de tipo información o servicios no necesita que se le asigne valor propio, pues éstos resultan valiosos en la medida en que soporten dichos activos esenciales.

En virtud de lo señalado, resultó necesario corregir la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3 expuesta por el Anexo A, para incluir, en la sección 5.3.3, las siguientes recomendaciones que surgieron como fruto de los hallazgos discutidos:

1. Se aconseja valorar únicamente los activos esenciales y dejar que el valor de los demás activos lo determine, automáticamente, la herramienta PILAR como el acumulado de los valores que éstos heredan de sus superiores a través de las dependencias.

2. Se sugiere que solamente se tenga en cuenta las dimensiones primarias: confidencialidad, disponibilidad e integridad.

- **Fallas en la valoración de las amenazas**

En la sección 6.1.2, mientras se valoraban las amenazas que atentaban contra los activos de información vinculados al caso de estudio, se logró identificar que la adaptación propuesta desconocía totalmente que, en [22], MAGERIT V3 declaraba que las amenazas no suelen materializarse sobre los activos esenciales sino, más bien, en los activos que los soportan, por lo cual, cualquier intento por identificar amenazas sobre los activos esenciales resultaría innecesario.

En virtud de lo señalado, se concluyó que, para conducir una adecuada gestión del riesgo de la SI en procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca, basta con caracterizar las amenazas que afectan los activos no esenciales.

Finalmente, la adaptación propuesta ignoró que, en la sección 8.6 del documento [22], MAGERIT V3 manifiesta que determinar la probabilidad de ocurrencia de las amenazas y la degradación causada sobre cada activo, en cada dimensión, es una tarea desmoralizadora y que, por lo cual, sugiere partir de datos estándar que sean ajustados hasta reflejar, con la mayor precisión posible, la realidad del caso de estudio.

Después de gestionar los riesgos de la SI en el caso de estudio, se determinó que tomar como referente los datos estándar de las amenazas suministrados por PILAR representa una opción viable, pues esta herramienta cuenta con una amplia trayectoria, uso y reconocimiento. Los criterios propuestos en la sección 5.3.4 fueron de gran ayuda para ajustar los valores de las amenazas, suministrados por PILAR, a las particularidades del contexto del caso de estudio como el nivel de conciencia y conocimiento en materia de la SI por parte del personal, a las condiciones climáticas de Popayán[75] y a las frecuentes interrupciones del suministro de energía a causa de las tormentas eléctricas, etc.

Por todo lo anterior, resultó necesario corregir la guía de recomendaciones sobre la adaptación de la metodología MAGERIT V3 expuesta por el Anexo A, para incluir, en la sección 5.3.4, las siguientes recomendaciones que surgieron como fruto de los hallazgos discutidos:

1. Se recomienda caracterizar, únicamente, las amenazas que atentan contra los activos no esenciales vinculados al procedimiento sobre el cual se vaya a gestionar los riesgos de la SI.

2. Se aconseja valorar las amenazas tomando, como punto de partida, los datos estándar de la biblioteca que provee la herramienta PILAR e ir ajustándolos a las particularidades del contexto del procedimiento sobre el cual se vaya a gestionar los riesgos de la SI.

[75] Por ejemplo, en la ciudad de Popayán se puede presentar una mayor probabilidad de que se materialicen amenazas como las inundaciones.

6.2.2. Evaluación de los expertos

Con el fin de reforzar la validación de la solución, la adaptación propuesta es sometida a la evaluación por parte de dos funcionarios de la Universidad del Cauca cuyas labores diarias involucran activamente la gestión de riesgos. En el Anexo D.1 se exponen las evidencias de la apreciación de cada uno de los expertos que, como resultado, terminaron formulando las siguientes correcciones para la adaptación:

1. El esquema para la clasificación de la información deberá demostrar el cumplimiento de las disposiciones emanadas por la Ley de Hábeas Data. La evaluadora sugiere realizar un mapeo entre la categorización propuesta por la adaptación y los tipos de datos que define la ley.

2. La organización para la gestión del riesgo, propuesta por la adaptación, debe incluir el área de Servidores y Servicios de Internet. La evaluadora argumenta que ésta área presta servicios que desempeñan un papel crítico en la mayoría de los procesos administrativos y académicos de la Universidad del Cauca.

3. Para el cálculo de la probabilidad de la amenaza se debe considerar la motivación (beneficios económicos por ejemplo) y el interés que tenga el atacante sobre la materialización de la amenaza.

4. Los criterios para la valoración de salvaguardas deben ser ajustados, pues el nivel de madurez L3 tiene un valor de eficacia muy alto. La evaluadora afirma que un procedimiento o control que esté documentado no es, necesariamente, eficiente en un 90%.

5. Los criterios para la valoración de los activos deben ser ajustados debido a que se le asigna un valor despreciable a la información pública. El evaluador argumenta que el hecho de que la información sea pública no quiere decir que sea prescindible o irrelevante.

6. Se debe verificar que los criterios para la valoración de amenazas, definidos por NIST, sean compatibles con la adaptación propuesta.

7. Los criterios para la evaluación del riesgo deben ser corregidos para que se considere activos críticos como el Sistema de Información de la VRI –SIVRI- y el sistema de archivo Satélite.

6.2.3. Indicadores

Según [98], un indicador es una expresión cualitativa o cuantitativa que permite evaluar el desempeño de cierto aspecto y determinar, de esa manera, el logro y cumplimiento de las metas propuestas. En virtud de lo señalado, conviene generar indicadores que permitan evaluar el desempeño de la adaptación como mecanismo para la gestión de riesgos de la SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca.

Frente a la amplia tipología de indicadores existentes, [98] establece una clasificación en las dimensiones de eficacia, eficiencia y efectividad.

- **Indicadores de eficacia**

Con este tipo de indicadores se va a medir el grado cumplimiento la meta principal de este proyecto: adaptar la metodología MAGERIT V3 al caso de estudio. En razón de lo expuesto se definen los siguientes indicadores:

I. **Indicador de innovación[76].** Busca medir la cantidad de elementos nuevos que introduce la adaptación propuesta con respecto a la versión original.

$$Innovación = \frac{Número\ de\ actividades\ nuevas}{Número\ total\ de\ actividades} * 100\% = \frac{8}{17} * 100\%$$

$$\boldsymbol{Innovación = 47\%}$$

Interpretación: casi la mitad (47%) de los componentes de la adaptación propuesta corresponde a nuevas actividades que fueron añadidas a la versión original de la metodología.

II. **Indicador de la adecuación lograda.** Este indicador pretende medir la cantidad de elementos, de la versión original, que fueron objeto de los ajustes formulados por la adaptación propuesta.

$$Adecuación = \frac{Número\ de\ actividades\ originales\ ajustadas}{Número\ de\ actividades\ originales} * 100\%$$

$$Adecuación = \frac{6}{9} * 100\%$$

$$\boldsymbol{Adecuación = 66\%}$$

[76] Partiendo de la siguiente definición de innovación: *cambio que introduce novedades.*

Interpretación: El 66% las actividades que MAGERIT V3 definía en su versión original fueron ajustadas y modificadas por la adaptación propuesta.

❖ **Indicadores de eficiencia**

Con este indicador se pretende medir la capacidad de la adaptación para lograr estimar y tratar los riesgos de la SI con el mínimo de recursos posibles o en el menor tiempo posible.

$$Eficiencia\ de\ la\ gestión = \frac{Número\ de\ riesgos\ tratados}{Número\ de\ días\ empleados} = \frac{186\ riesgos\ tratados}{9\ días}$$

$$\boldsymbol{Eficiencia\ de\ la\ gestión = 21\ riesgos\ tratados/día}$$

Interpretación: Aplicando la adaptación propuesta se logró estimar y tratar satisfactoriamente todos los riesgos en el caso de estudio a una razón de 21 riesgos por día.

❖ **Indicadores de efectividad**

Con este indicador se pretende medir el impacto que tiene la adaptación en la gestión de riesgos de la SI para el caso de estudio propuesto. Para ello, se van a formular los siguientes indicadores:

I. **Impacto a la mitigación de riesgos.** Pretende medir el grado con el cual la adaptación logra tratar los riesgos hasta reducirlos a niveles despreciables.

$$Mitigación = \frac{Nivel\ de\ riesgo\ promedio\ inicial - Nivel\ de\ riesgo\ promedio\ final}{Nivel\ de\ riesgo\ promedio\ inicial} * 100\%$$

$$Mitigación = \frac{3{,}4 - 0{,}2}{3{,}4} * 100\%$$

$$\boldsymbol{Mitigación = 94\%}$$

Interpretación: La adaptación propuesta logró reducir el nivel de riesgo inicial en un 94%.

II. Indicador de satisfacción al cliente. Pretende determinar el grado de aceptación de la adaptación por parte del usuario, quien corresponde al Jefe de la División de Gestión de Investigación; el señor Helder Mauricio Chacón. Para ello, se realizó una encuesta con base en la escala de Likert, tal y como lo evidencia el Anexo D.2, en la cual se le pregunta al usuario por su grado de satisfacción en ciertos aspectos de la metodología.

Escala de Likert		
Valor respuesta	**Respuesta**	**Satisfacción**
5	Totalmente de acuerdo	Completamente satisfecho
4	De acuerdo	Altamente satisfecho
3	Parcial	Satisfecho
2	En desacuerdo	Insatisfecho
1	Totalmente en desacuerdo	Completamente insatisfecho

Tabla 6.3. Escala de Likert [97]

$$Satisfacción\ al\ cliente = \sum_{i=1}^{12} \frac{ValorRespuesta_i}{12}$$

$$\boldsymbol{Satisfacción\ al\ cliente = 5}$$

Interpretación: La adaptación propuesta logró obtener un grado de satisfacción al cliente de 5 puntos, lo que, de acuerdo con la Tabla 6.3, se traduce en una completa satisfacción del usuario de la adaptación.

Conclusiones

Al finalizar el presente proyecto, se concluye que la metodología MAGERIT V3 se logró adaptar como un mecanismo adecuado para la gestión de riesgos de la SI en procedimientos, que como el caso de estudio, están dirigidos a gestionar proyectos de investigación en la Universidad del Cauca.

En relación con lo anterior, en tempranas etapas del proyecto se encontró que la metodología MAGERIT V3 presenta varias deficiencias con respecto a los artefactos requeridos por los estándares para una adecuada gestión del riesgo. En consecuencia, para poder adaptar esta metodología y superar las insuficiencias detectadas, fue necesario agregar 8 nuevas actividades al enfoque definido por MAGERIT V3 en su versión original, obteniendo como resultado el Método de Análisis de Riesgos Adaptado –MARA.

Respecto a lo anterior, se resalta que la mayoría de las nuevas actividades están encaminadas a definir criterios que permitan obtener valoraciones precisas, objetivas, realistas e independientes de la arbitrariedad del analista. En este aspecto, la metodología NIST desempeña un papel fundamental al proveer criterios ampliamente aprobados por la comunidad científica y que resultaron ser completamente compatibles con la adaptación propuesta.

De esta manera, el Método de Análisis de Riesgos Adaptado –MARA, formaliza el conjunto de actividades necesarias para poder adaptar MAGERIT V3 al caso de estudio, indicando de manera clara el *qué se debe hacer.* Para aclarar el *cómo hacerlo,* la guía de recomendaciones suministra al usuario instrucciones claras sobre el uso de la adaptación y la ejecución de cada una de las actividades definidas por la misma.

Con el MARA y su respectiva guía de aplicación, se logró un enfoque para la gestión de riesgos que a diferencia del propuesto por MAGERIT V3:

- No incumple los requerimientos establecidos por la norma ISO/IEC 27001, garantizando que, primero, se valoren y prioricen los riesgos para que luego se seleccionen los controles para su respectivo tratamiento.

- Sí satisface los artefactos requeridos por los estándares.

- Sí se encuentra ajustado y alineado al contexto de los procedimientos que, como el caso de estudio, están dirigidos a gestionar proyectos de investigación en la Universidad del Cauca.

Gracias al uso de la adaptación propuesta se logró:

- Determinar que, en el caso de estudio, se cuenta con activos muy valiosos.
- Identificar que los activos, vinculados al caso de estudio, se encuentran expuestos a variadas amenazas.
- Determinar que, en el caso de estudio, se carece de los controles necesarios para hacer frente a las amenazas de la SI.
- Identificar que el caso de estudio se encuentra sometido a un alto nivel de riesgos de la SI.
- Mitigar en un 94% los riesgos a los que se encontraba expuesto el caso de estudio a una razón de 24 riesgos por día.
- Reducir todos los riesgos hasta niveles despreciables

Para terminar, cabe recordar que el desarrollo del proyecto se llevó a cabo usando la metodología del Ingeniero Carlos Serrano. Aunque se logró un desarrollo sistemático, con éste método no se lograba garantizar la continua y activa participación del usuario en la construcción de la solución. En razón de lo expuesto y con el propósito de generar una solución de calidad, resultó necesario incluir al usuario de la adaptación, el jefe de la División de Gestión de Investigación, en todas las etapas de desarrollo del proyecto.

Bibliografía

[1] Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO/IEC 27000, 2014

[2] Information Technology – Security techniques -- Information security management systems — Requirements, ISO/IEC 27001, 2013.

[3] Information technology — Security techniques — Code of practice for information security controls, ISO/IEC 27002, 2013

[4] Information Technology -- Security techniques -- Information security management system implementation guidance, ISO/IEC 27003, 2010.

[5] Information Technology — Security techniques — Information security risk management, ISO/IEC 27005, 2011.

[6] P. Pastor y M. Francisco, “Gestión y control de procesos,” en Reflexiones para implementar un sistema de gestión de calidad (ISO 9001:2000), primera Ed, Bogotá, Colombia, 2007, Cap. 4, pp. 50-51.

[7] M. José, “La mejora gradual de los procesos,” en Guía Metodológica para la Gestión Clínica por Procesos, Primera ed, España, Madrid, Ediciones Diaz de Santos S.A., 2003, cap. 9, pp. 341-343.

[8] M. Francisco, C. Antonio, R. Sergio, “La filosofía de los gurús de la calidad,” en Introducción a la gestión de la calidad, primera ed., Las Rozas, Madrid, Delta Publicaciones universitarias, 2007, Cap. 2, pp. 35-36.

[9] "Círculo de Deming", *es.wikipedia.org*, 2016. [Online]. Available: https://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming. [Accessed: 30-Mar-2016].

[10] Foro de implementación ISO 27k, "ISO27k_ISMS_implementation_and_certification_process_v3_Spanish," ISO27k infosec management standards, January 2009 [PDF]. Available: http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process_v3_Spanish.pdf. [Accessed: 30-MAR-2016].

[11] Centro Criptológico Nacional de España. 2015, March 13. PILAR 5.4.5 [Software]. Available: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/pilar.html.

[12] M. Juan y E. Diego, “Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S. Caso de estudio: Proceso de Inscripciones y Admisiones en la División de Admisión Registro y Control Académico (DARCA) de la

Universidad del Cauca," Trabajo de pregrado, Universidad del Cauca, Cauca, Colombia, 2014.

[13] A. Alexander, *Diseño de un sistema de gestión de seguridad de información*. Bogotá: Alfaomega Colombiana, 2007.

[14] NORTH ATLANTIC TREATY ORGANISATION –NATO-OTAN, "Improving Common Security Risk Analysis," Tech. Rep. AC/323(IST-049) TP/193, Sep. 2008.

[15] C. Jonathan, "Risk management in methodologies of information technology and communications projects," Enfoque UTE. Rev., V.4-N.2, pp. 77 - 94, Dec. 2013.

[16] L. Chang and Z. Lee, "Applying fuzzy expert system to information security risk Assessment - A case study on an attendance system", 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY), pp. 345-351, 2013.

[17] A. Tamjidyamcholo, "Information security risk reduction based on genetic algorithm", Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 122-127, 2012.

[18] R. Montesino and S. Fenz, "Automation Possibilities in Information Security Management", 2011 European Intelligence and Security Informatics Conference, pp. 259-262, 2011

[19] L. Antonio and V. John, "Análisis y gestión de riesgos de los sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología Magerit," Trabajo de pregrado, Universidad de Cuenca, Cuenca, Ecuador, 2012.

[20] R. Edison, "Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la contraloría general del estado," Trabajo de pregrado, Universidad Central Del Ecuador, Quito, Ecuador, 2014.

[21] P. John y C. Mildred, "Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca," Trabajo de especialización en seguridad informática, UNAD, Popayán, Cauca, 2014.

[22] A. Ana, P. Jarol, B. John, "Análisis de riesgos en la seguridad de la información", Trabajo de investigación en especialización, Fundación Universitaria Juan de Castellanos, Tunja, Colombia 2013.

[23] *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*, 1st ed. Madrid: Ministerio de Hacienda y Administraciones Públicas, Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones, Centro de Publicaciones, 2012, pp. 6-127.

[24] *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*, 1st ed. Madrid: Ministerio de Hacienda y Administraciones Públicas, Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones, Centro de Publicaciones, 2012, pp. 6-75.

[25] *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas*, 1st ed. Madrid: Ministerio de Hacienda y Administraciones Públicas, Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones, Centro de Publicaciones, 2012, pp. 4-42.

[26] C. Serrano, “Modelo para la construcción de soluciones,” en *Modelo Integral para el Profesional en Ingeniería*, primera Ed., Popayán, Colombia, Editorial Universidad del Cauca, 2005, Cap. 4, Sec. 2, pp. 84-90.

[27] "Consulta de la Norma: ley 872 de 2003", *Alcaldiabogota.gov.co*, 2016. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=11232. [Accessed: 02- Apr- 2016].

[28] Norma técnica de calidad en la gestión pública, NTCGP 1000, 2009.

[29] Modelo estándar de control interno para el estado colombiano, MECI 1000:2005, 2005.

[30] Gestión de Recursos Tecnológicos » Blog Archive » Resolución R802 de 2011", *Ublogs.unicauca.edu.co*, 2016. [Online]. Available: http://ublogs.unicauca.edu.co/sgc-tics/resolucion-r802-de-2011/. [Accessed: 02- Apr- 2016].

[31] *Manual de la Calidad*, versión 3. Popayán: Área Sistema Integrado Gestión de la calidad, September 2015 [PDF]. Available: http://facultades.unicauca.edu.co/prlvmen/sites/default/files/procesos/PE-GS-2.2.1-MN-1%20Manual%20de%20calidad.pdf. [Accessed: 02-Apr-2016].

[32] *Caracterización Proceso Gestión de la Investigación*, versión 3. Popayán: Área Sistema Integrado Gestión de la calidad, March 2015 [PDF]. Available: http://facultades.unicauca.edu.co/prlvmen/sites/default/files/documentos/caracterizacion/PM-IV-6-CA%20Gesti%C3%B3n%20de%20la%20investigaci%C3%B3n..pdf. [Accessed: 02-Apr-2016].

[33] *Formulación y ejecución de proyectos con financiación externa*, versión 1. Popayán: Área Sistema Integrado Gestión de la calidad, September 2015 [PDF]. Available: http://facultades.unicauca.edu.co/prlvmen/sites/default/files/procesos/PM-IV-6.1-PR-3%20Formulaci%C3%B3n%20y%20ejecuci%C3%B3n%20de%20proyectos%20con%20financiaci%C3%B3n%20externa_0.pdf. [Accessed: 02-Apr-2016].

[34] *Formulación y ejecución de proyectos con financiación externa*, versión 1. Popayán: Área Sistema Integrado Gestión de la calidad, September 2015 [PDF]. Available: http://facultades.unicauca.edu.co/prlvmen/sites/default/files/procesos/PM-IV-6.1-PR-3%20Formulaci%C3%B3n%20y%20ejecuci%C3%B3n%20de%20proyectos%20con%20financiaci%C3%B3n%20externa_0.pdf. [Accessed: 02-Apr-2016].

[35] "Resolución R-785 de 2015 (política del Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca)", *unicauca.edu.co*, 2015. [Online]. Available: http://www.unicauca.edu.co/versionP/documentos/resoluciones/resoluci%C3%B3n-r-785-de-2015-sistema-de-seguridad-de-la-informaci%C3%B3n-de-la-universidad-del-cauca. [Accessed: 06- Apr- 2016].

[36] "Consulta de la Norma: ley 527 de 1999", *Alcaldiabogota.gov.co*, 2016. [Online]. Available:

http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276. [Accessed: 02- Apr- 2016].

[37] "Consulta de la Norma: ley estatutaria 1266 de 2008", *Alcaldiabogota.gov.co*, 2016. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488. [Accessed: 02- Apr- 2016].

[38] "Consulta de la Norma: ley estatutaria 1581 de 2012", *Alcaldiabogota.gov.co*, 2016. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Accessed: 02- Apr- 2016].

[39] "Consulta de la Norma: decreto 1377 de 2013", *Alcaldiabogota.gov.co*, 2016. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [Accessed: 02- Apr- 2016].

[40] "Acuerdo Nº 064 de 2008 (Estatuto de Contratación de la Universidad del Cauca)", *unicauca.edu.co*, 2015. [Online]. Available: http://portal.unicauca.edu.co/versionP/documentos/acuerdos/acuerdo-no-064-de-2008. [Accessed: 06- Apr- 2016].

[41] "Acuerdo Superior 015 de 2015 (establecimiento del Sistema de Investigaciones de la Universidad del Cauca)", *unicauca.edu.co*, 2015. [Online]. Available: http://www.unicauca.edu.co/versionP/documentos/acuerdos/acuerdo-superior-015-de-2015-establecimiento-del-sistema-de-investigaciones-de-la-universidad-del-ca. [Accessed: 06- Apr- 2016].

[42] "Consulta de la Norma: ley 1712 de 2014", *Alcaldiabogota.gov.co*, 2016. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=568. [Accessed: 02- Apr- 2016].

[43] *Guía para la calificación de la información de acuerdo con sus niveles de seguridad*, versión 4. Bogotá D.C: Presidencia de la República de Colombia, April 2015 [PDF]. Available: http://wp.presidencia.gov.co/sitios/dapre/sigepre/guias/G-GD-02%20Gu%C3%ADa%20para%20la%20Clasificaci%C3%B3n%20de%20la%20Informaci%C3%B3n.pdf. [Accessed: 02-Apr-2016].

[44] A. S. Sendi, M. Jabbarifar, M. Shajari, and M. Dagenais, "FEMRA: Fuzzy Expert Model for Risk Assessment," in *Internet Monitoring and Protection (ICIMP)*, 2010 Fifth International Conference on, 2010, pp. 48-53.

[45] M. Meng, "The research and application of the risk evaluation and management of information security based on AHP method and PDCA method," in *Information Management, Innovation Management and Industrial Engineering (ICIII)*, 2013 6th International Conference on, 2013, pp. 379-383.

[46] F. Sha and Z. Hangjun, "The information security risk assessment based on AHP and fuzzy comprehensive evaluation," in *Communication Software and Networks (ICCSN)*, 2011 IEEE 3rd International Conference on, 2011, pp. 124-128.

[47] K.V.D.Kiran, L.S.S.Reddy and N.Lakshmi Haritha, "A Comparative Analysis on Risk Assessment Information Security Models," *International Journal of Computer Applications*, Volume 82 – No.9, November 2013.

[48] *Manual de usuario PILAR: análisis y gestión de riesgos,* versión 5.4. Madrid: Ministerio de la Presidencia del Gobierno de España y el Centro Criptológico Nacional, August 2014 [PDF]. Available: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/470G/470G1_Manual_de_usuario_Pilar_analisis_y_gestion_de_riesgos.pdf. [Accessed: 02-Apr-2016].

[49] "Inicio - Estrategia GEL", *Estrategia.gobiernoenlinea.gov.co*, 2016. [Online]. Available: http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html. [Accessed: 07- Apr- 2016].

[50] "CSIRT-CCIT", *Csirt-ccit.org.co*, 2016. [Online]. Available: http://www.csirt-ccit.org.co/index.html. [Accessed: 07- Apr- 2016].

[51] *Guía de seguridad CCN-STIC-803: Esquema nacional de seguridad valoración de los sistemas,* versión 1. Madrid: Ministerio de Defensa de España, January 2011 [PDF]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html. [Accessed: 02-Apr-2016].

[52] *NIST Special Publication 800-30: Guide for Conducting Risk Assessments*, Revision 1. Gaithersburg: National Institute of Standards and Technology - NIST, September 2012 [PDF]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. [Accessed: 02-Apr-2016].

[53] *Manual de usuario PILAR,* versión 5.1. Madrid: Ministerio de defensa del Gobierno de España y el Centro Criptológico Nacional, May 2011 [PDF]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/152-ccn-stic-470d-manual-de-la-herramienta-de-analisis-de-riesgos-pilar-5-1/file.html. [Accessed: 02-Apr-2016].

[54] *Guía de gestión de riesgos,* versión 2. Bogotá D.C: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, November 2010 [PDF]. Available: http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Riesgo.pdf. [Accessed: 02-Apr-2016]

[55] *criteria_es.xml,* versión 1. Popayán: Galindez M, Reyes J. April 2016 [XML]. Available: https://drive.google.com/file/d/0BwSRPC5EmhRIWnh6QW5uUlZCMmc/view?usp=sharing. [Accessed: 18-Apr-2016].

[56] *Riesgo residual en el procedimiento de Formulación y ejecución de proyectos con financiación externa - VRI,* versión 1. Popayán: Galindez M, Reyes J. April 2016 [DOCX]. Available: https://drive.google.com/file/d/0BwSRPC5EmhRIb19icGtLa3d5ZW8/view?usp=sharing. [Accessed: 18-Apr-2016].

[57] "Consulta de la Norma: decreto 19 de 2012", *Alcaldiabogota.gov.co*, 2016. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [Accessed: 02- Apr- 2016].

[58] *Reporte de incidente de seguridad de la información*, versión 1. Buenos Aires, Argentina: Departamento de seguridad informática de la Universidad Nacional de Luján [PDF]. Available:

http://www.unlu.edu.ar/doc/seginfo/Como_reportar_un_incidente_de_SI.pdf. [Accessed: 02-Apr-2016].

[59] *Reporte de incidente de seguridad informática*, versión 1. México D.F: Departamento de seguridad en cómputo de la Universidad Nacional Autónoma de México [PDF]. Available: http://redyseguridad.fi-p.unam.mx/proyectos/politicas/desc/formato_reporte.pdf. [Accessed: 02-Apr-2016].

[60] M. Montesi and P. Lago, "Software engineering article types: An analysis of the literature", *Journal of Systems and Software*, vol. 81, no. 10, pp. 1694-1714, 2008.

[61] M. Zelkowitz and D. Wallace, "Experimental models for validating technology", *Computer*, vol. 31, no. 5, pp. 23-31, 1998.

[62] R. Yin, “How to Know Whether and When to Use Case Studies as a Research Method,” in *Case study research, Fourth Edition*. Los Angeles, Calif.: Sage Publications, 2009, ch. 1, pp. 11–12.

[63] C. Wohlin, "An analysis of the most cited articles in software engineering journals - 2000", *Information and Software Technology*, vol. 49, no. 1, pp. 2-11, 2007.

[64] T. DINGSØYR and R. CONRADI, "A SURVEY OF CASE STUDIES OF THE USE OF KNOWLEDGE MANAGEMENT IN SOFTWARE ENGINEERING", *Int. J. Soft. Eng. Knowl. Eng.*, vol. 12, no. 04, pp. 391-414, 2002.

[65] D. Sjoeberg, J. Hannay, O. Hansen, V. Kampenes, A. Karahasanovic, N. Liborg and A. Rekdal, "A survey of controlled experiments in software engineering", *IEEE Transactions on Software Engineering*, vol. 31, no. 9, pp. 733-753, 2005.

[66] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering", *Empirical Software Engineering*, vol. 14, no. 2, pp. 131-164, 2008.

[67] B. Kitchenham, S. Pfleeger, L. Pickard, P. Jones, D. Hoaglin, K. El Emam and J. Rosenberg, "Preliminary guidelines for empirical research in software engineering", *IEEE Transactions on Software Engineering*, vol. 28, no. 8, pp. 721-734, 2002.

[68] M. Goncalves, C. de Souza and V. Gonzalez, "Initial findings from an observational study of software engineers", *2009 13th International Conference on Computer Supported Cooperative Work in Design*, 2009.

[69] J. Wu, T. Graham and P. Smith, "A study of collaboration in software design", *2003 International Symposium on Empirical Software Engineering, 2003. ISESE 2003. Proceedings.*

[70] C. Wohlin, M. Höst and K. Henningsson, "Empirical Research Methods in Software Engineering", *Empirical Methods and Studies in Software Engineering*, pp. 7-23, 2003.

[71] T. Dybå and T. Dingsøyr, "Strength of evidence in systematic reviews in software engineering", *Proceedings of the Second ACM-IEEE international symposium on Empirical software engineering and measurement - ESEM '08*, pp. 178-187, 2008.

[72] L. Pickard, B. Kitchenham and P. Jones, "Combining empirical results in software engineering", *Information and Software Technology*, vol. 40, no. 14, pp. 811-821, 1998.

[73] *Anteproyecto de Trabajo de Grado: Gestión del riesgo de SI con base en la norma ISO/IEC 27005:2011 adaptando la metodología MAGERIT V3 para el caso de estudio propuesto,* versión 1. Popayán: Galindez M, Reyes J. April 2016 [PDF]. Available: https://drive.google.com/file/d/0BwSRPC5EmhRILXNnM0UzSFNaVFU/view?usp=sharing. [Accessed: 18-Apr-2016].

[74] *Excel 2013*. Microsoft Corporation, 2013.

[75] *Word 2013*. Microsoft Corporation, 2013.

[76] "Formstack's Form Builder Solution | Online Forms + Powerful Features", *Formstack.com*, 2016. [Online]. Available: https://www.formstack.com/. [Accessed: 16- May- 2016].

[77] Khan SU, Niazi M. "Systematic Literature Review Protocol for Software Outsourcing Vendors Readiness Model (SOVRM). TR/08- 01," School of Computing and Maths, Keele University,UK 2008.

[78] Khan SU, Niazi M, Ikram N. "Systematic Literature Review Protocol for Software Outsourcing Relationships Trust (SORT). TR/2009-01," School of Computing and Maths, Keele University, UK 2009:40.

[79] Beecham S, Baddoo N, Hall T, Robinson H, Sharp H. "Protocol for a Systematic Literature Review of Motivation" in *Software Engineering*. School of Computer Science, University of Hertfordshire, College Lane Campus, Hatfield, Hertfordshire AL10 9AB 2006:87.

[80] Turner M, Charters S. "Protocol for a Systematic Literature Review of the Technology Acceptance Model and its Predictive Capabilities", Keele University, UK; 2006.

[81] Rabbi "A Systematic Literature Review Protocol," in *IOSR Journal of Computer Engineering (IOSRJCE)*, Volume 2, Issue 2(July-Aug. 2012), PP 23-29.

[82] D. Milicevic and M. Goeken, "Application of models in information security management," in *Research Challenges in Information Science (RCIS)*, 2011 Fifth International Conference on, 2011, pp. 1-6.

[83] G. Pavlov and J. Karakaneva, "Information security management system in organization," *Trakia Journal of Sciences*, vol. 9, pp. 20-25, 2011.

[84] [27] A. Asosheh, P. Hajinazari, and H. Khodkari, "A practical implementation of ISMS," in *e-Commerce in Developing Countries: With Focus on e-Security (ECDC)*, 2013 7th Intenational Conference on, 2013, pp. 1-17.

[85] B. Karabacaka, and I. Sogukpinar, "ISRAM: information security risk analysis method". Computers and Security Volume 2003 24, pp. 147 -159.

[86] M. Moyo, H. Abdullah, and R. C. Nienaber, "Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems," in *Information Security for South Africa*, 2013, 2013, pp. 1-6.

[87] V. Lalanne, M. Munier, and A. Gabillon, "Information Security Risk Management in a World of Services," in *Social Computing (SocialCom)*, 2013 International Conference on, 2013, pp. 586-593.

[88] H. Ying, C. Johnson, K. Renaud, L. Yu, and S. Jebriel, "An empirical study on the use of the Generic Security Template for structuring the lessons from information security incidents," *in Computer Science and Information Technology (CSIT)*, 2014 6th International Conference on, 2014, pp. 178-188.

[89] V. Gonzalo, “Armonización de múltiples modelos para el análisis de riesgos de las tecnologías de la información y desarrollo de software,” Tesis de pregrado, Universidad San Buenaventura, Cali, Colombia 2013.

[90] V. Gonzalo, P. César, “Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT,” *Revista S&T*, 12(30), 35-48, Universidad Icesi, Cali, Colombia 2014.

[91] C. Fernando, P. Bertulfo, “Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización,” Tesis de Maestría, Universidad Icesi, Cali, Colombia 2012.

[92] Vicerrectoría de Investigaciones, "Directorio", *VRI - Universidad del Cauca*. [Online]. Available: http://vri.unicauca.edu.co:8081/vri2011/index.php/vri/directorio. [Accessed: 23- May- 2016].

[93] *Entrevistas y encuestas para el proyecto de gestion de riesgos de SI en un procedimiento de la VRI,* versión 1. Popayán: Galindez M, Reyes J. April 2016 [PDF]. Available: https://drive.google.com/folderview?id=0BwSRPC5EmhRIX3VVYmJETjYzT00&usp=sharing. [Accessed: 18-Apr-2016].

[94] A. Carina, R. Per, “Verification and Validation in Industry, A Qualitative Survey on the State of Practice”, Lund University, Lund, Sweden, 2002.

[95] X. Wang, X. Wu, “Study of Methodology of E-business Survey and Analysis”, Jiangsu Institute of Education, Nanjing, China, 2012.

[96] V. Maria, “Metodología de desarrollo de modelos de calidad orientados a dominio y su aplicación al dominio de los productos finales de seguridad de tecnologías de la información”, Universidad de Alcalá, Alcalá de Henares, España, 2009.

[97] R. Ravi, S. Haritima , R. Bharath, “Survey on Application Level Tools for SSD Benchmark Validation”, Mahindra Satyam, Telangana, India, 2013.

[98] Likert, R. "The method of constructing an attitude scale", Archives of Psychology, New York, USA, 1932, pp. 44–53.

[99] Departamento Administrativo de la Función Pública, *Guía para la construcción de indicadores de gestión*, 2nd ed. Bogotá: Elizabeth Rodriguez Taylor, 2016, pp. 17-30.

Anexo A

Políticas de la SI para el caso de estudio

A.1. Política de tratamiento y protección de datos personales

Objetivo: definir las pautas generales para el tratamiento y protección de datos personales con el fin de dar cumplimiento a lo estipulado por la ley estatutaria 1581 de 2012 [37] y su decreto reglamentario 1377 de 2013 [38].

Directrices: la VRI, en su calidad de *Responsable* y *Encargado* del tratamiento de datos personales, observará y aplicará los distintos principios rectores estipulados por el artículo 4 de la ley 1581 de 2012.

La VRI, en cumplimiento del artículo 6 de la ley 1581 de 2012, realizará el Tratamiento de datos sensibles, solo cuando:

a. El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

b. El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

c. El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En

estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

d. El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

e. El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

De acuerdo a lo estipulado por el artículo 10 de la ley 1581 de 2012, la VRI da a conocer, al público en general, los casos, en los cuales, no es necesaria la autorización del Titular para el tratamiento de su información:

a. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
b. Datos de naturaleza pública.
c. Casos de urgencia médica o sanitaria.
d. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
e. Datos relacionados con el Registro Civil de las personas.

Dando cumplimiento al artículo 13 de la ley 1581 de 2012, la VRI, suministrará la información personal únicamente a:

a) Los Titulares, sus causahabientes o sus representantes legales.
b) Las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
c) Los terceros autorizados por el Titular o por la ley 1581 de 2012.

La VRI, en su calidad de *Responsable* y *Encargado* del tratamiento de datos personales, reconoce su deber de:

a. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data. En consecuencia, adquiere el deber de observar y cumplir las disposiciones de la ley 1266 de 2008.
b. Solicitar y conservar copia de la respectiva autorización otorgada por el Titular
c. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada
d. Informar a solicitud del Titular sobre el uso dado a sus datos
e. **Conservar la información bajo las condiciones de seguridad necesarias** para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

f. Garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.
g. Abstenerse de tratar información de la cual no se tenga previa autorización del titular (conforme lo previsto en la ley 1581 de 2012).
h. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
i. Realizar oportunamente la actualización, rectificación o supresión de los datos.
j. Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la ley 1581 de 2012.
k. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio
l. Tramitar las consultas y reclamos formulados en los términos señalados en la ley 1581 de 2012.
m. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley 1581 de 2012 y en especial, para la atención de consultas y reclamos
n. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
o. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
p. La VRI hará uso de los datos personales del titular solo para aquellas finalidades para las que se encuentre debidamente facultada y respetando en todo caso la normatividad vigente sobre protección de datos personales.
q. Observar y aplicar las demás disposiciones de la ley estatutaria 1581 de 2012 y su Decreto Reglamentario 1377 de 2013.

La VRI, en su calidad de *Responsable* y *Encargado* del tratamiento de datos personales, se compromete a cumplir los siguientes derechos que, por disposiciones de la ley 1581 de 2012, le asisten al titular de la información:

a. Conocer, actualizar y rectificar sus datos personales frente a la VRI. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

b. Solicitar prueba de la autorización otorgada a la VRI, salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012.

c. Ser informado por la VRI, previa solicitud, respecto del uso que le ha dado a sus datos personales.

d. Presentar, ante la Superintendencia de Industria y Comercio, quejas por infracciones a lo dispuesto en la ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.

e. Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

f. Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

A.2. Política sobre el uso de la criptografía

Objetivo: definir las pautas generales para garantizar el apropiado y efectivo uso de la criptografía con el fin de lograr:

1. **Confidencialidad:** usando algoritmos criptográficos se logra proteger la información crítica o sensible que es almacenada o transmitida.
2. **Integridad/autenticidad:** usando firmas digitales o códigos de autenticación de mensajes se logra verificar la integridad y autenticidad de la información crítica o sensible que es almacenada o transmitida.
3. **No repudiación:** usando técnicas criptográficas para proveer la evidencia de la ocurrencia o no ocurrencia de un evento o una acción.
4. **Autenticación:** usando técnicas criptográficas para autenticar usuarios y entidades que solicitan acceso a los activos de información.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Usar mecanismos criptográficos para proteger la información transportada por la red o en dispositivos de almacenamiento móviles o removibles.
b. Definir roles y responsabilidades sobre el uso de la criptografía.
c. Evaluar el impacto del cifrado de la información sobre los controles de inspección[77].

[77] Por ejemplo: el detector de malware no podrá analizar la información cifrada a menos que posea la clave y el acceso al algoritmo criptográfico usado para la operación de cifrado.

d. Establecer e implementar un enfoque para la gestión de claves criptográficas, incluyendo métodos para la recuperación de la información cifrada en caso de pérdida, compromiso o daño de las claves.
e. Reconocer la firma digital como un elemento jurídico que tiene la misma fuerza y efectos que la firma manuscrita, siempre y cuando incorpore los siguientes atributos[78]:
    1. Es única a la persona que la usa.
    2. Es susceptible de ser verificada.
    3. Está bajo el control exclusivo de la persona que la usa.
    4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
    5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

f. Obtener las firmas digitales por parte de entidades de certificación que cumplan con los requerimientos y sean acreditados por el Organismo Nacional de Acreditación conforme a la reglamentación expedida por el Gobierno Nacional[79].
g. Garantizar que los suscriptores de las firmas digitales son conscientes de sus deberes y responsabilidades conforme a lo estipulado por la ley 527 DE 1999 [35].

A.3. Política de control de acceso

Objetivo: definir las pautas generales para garantizar el registro, identificación y autenticación de los usuarios, a fin de garantizar el acceso limitado y controlado a los activos de información.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

- Definir las reglas de acceso a los activos de información con base en la premisa de **denegación por defecto**[80].

[78] Por disposición del artículo 28 de la ley 527 DE 1999 [35].
[79] Por disposición del artículo 160 del Decreto Nacional 019 de 2012 [56], mediante el cual se modifica el artículo 29 de la ley 527 DE 1999.
[80] "*Por defecto, todo está prohibido, a menos que sea, explícitamente, permitido*".

- Otorgar el acceso, físico o lógico, a los activos de información solamente a los usuarios que estén explícitamente autorizados.
- Controlar el acceso a sistemas y aplicaciones que procesan, almacenan o recuperan información sensible mediante un proceso seguro de "*inicio de sesión"* que realice una fuerte autenticación y verificación de la identidad del usuario.
- Restringir el acceso al código fuente del software usado
- Exigirle a los propietarios de los activos la segregación de los roles para el control de acceso.
- Determinar las reglas de control de acceso a los activos y las restricciones para usuarios específicos.
- Implementar un proceso formal para el registro de usuarios a fin de habilitar la asignación de derechos de acceso a los activos de información. El proceso de registro asignará un identificador único a cada usuario para vincularlo al sistema y hacerlo responsable de sus acciones. El uso de identificadores compartidos solo será permitido cuándo y dónde sea estrictamente necesario.
- Controlar la asignación de la información secreta de autenticación[81] a través de un proceso formal. Se garantizará que la información temporal de autenticación será única para cada usuario, que no será predecible y que se entregará al usuario de manera segura[82].
- Implementar un proceso formal para la asignación y revocación de los derechos de acceso a los activos de información. Los derechos serán concedidos al identificador único de cada usuario. Se verificará que los derechos de acceso no sean activados antes de que el proceso de autorización se haya completado.
- Controlar y restringir el uso y asignación de derechos de acceso privilegiado a través de un proceso formal de autorización, los cuales serán asignados a identificadores de usuario diferentes de los usados para las actividades regulares.
- Mantener un registro centralizado de los derechos de acceso concedidos a los usuarios. Los propietarios de los activos de información tendrán la responsabilidad de revisar los derechos de acceso a intervalos planeados o cuando cualquier cambio ocurra (por ejemplo: nueva contratación, terminación del empleo, cambios en los roles de usuario, etc.).
- Remover o suspender, inmediatamente, los identificadores de los usuarios (empleados y partes externas) que ya no estén vinculados al caso de estudio.

[81] Algunos ejemplos de información secreta de autenticación son las contraseñas, claves criptográficas, tarjetas inteligentes, etc.
[82] Por ejemplo, las contraseñas NO se deben enviar en texto claro por correo electrónico o mensaje de texto.

- Remover o suspender, inmediatamente, los derechos de acceso de los usuarios (empleados y partes externas) que ya no estén vinculados a al caso de estudio.

A.4. Política para la clasificación de la información.

Objetivo: definir las pautas generales para garantizar que la información recibe un nivel de protección apropiado acorde a su importancia.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

- Definir un esquema para la clasificación de la información gestionada por el caso de estudio. Dicho esquema estará alineado con las directrices emanadas por la ley 1712 de 2014 [41].
- Responsabilizar de la clasificación de la información a los propietarios de los activos.
- Categorizar los demás activos de acuerdo a la clasificación de la información que éstos almacenan, procesan, manipulan o protegen.
- Definir e implementar procedimientos para el etiquetado y manipulación de activos de información de acuerdo con el esquema de clasificación definido.
- Definir e implementar los controles necesarios para garantizar la protección de los activos de información de acuerdo con su clasificación.
- Definir e implementar procedimientos que le permitan a los entes externos identificar e interpretar la clasificación de la información que se comparte con ellos.

A.5. Política de seguridad física

Objetivo: definir las pautas generales para prevenir el acceso no autorizado a las instalaciones físicas de la organización, el daño e interferencia a la información, principalmente a zonas en donde se almacene y procese información.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Proteger las áreas en donde se encuentre almacenada la información, considerada como crítica o confidencial, mediante la definición de perímetros de seguridad, controles de acceso físicos para funcionarios y personas externas al caso de estudio.
b. Restringir el acceso físico a las oficinas, salas, instalaciones, y demás áreas en donde se encuentren activos de información importantes, permitiendo el acceso únicamente a personas autorizadas.
c. Diseñar y aplicar protección física a los equipos de la organización contra desastres ambientales, ofensivas maliciosas, fallos de suministro o posibles accidentes que atenten contra la integridad de los mismos.
d. Construir y aplicar procedimientos para la realización de reuniones y trabajo, tomando medidas como: no permitir el ingreso de dispositivos que registren las actividades del caso de estudio, y que dichas actividades sean privadas o confidenciales.
e. Impedir el retiro de equipos de información y/o software de su lugar sin autorización previa por parte del personal encargado de estos activos de la organización.

A.6. Política de copias de respaldo

Objetivo: definir las pautas generales para garantizar una adecuada protección contra pérdida de datos.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Realizar copias, completas y precisas, de la información, software e imágenes de sistemas. Las copias de seguridad serán ubicadas, en lo posible, en una localización remota, lo suficientemente distante como para escapar de cualquier daño sufrido en los sistemas operacionales.
b. Proveer instalaciones de backup adecuadas para garantizar que toda la información y software esencial puedan ser recuperados después de un fallo o desastre. Dichas instalaciones serán protegidas de acuerdo con lo establecido por la **política de seguridad física**[83].

[83] Ver Anexo A.5

c. Definir e implementar procedimientos documentados para el proceso de restauración de la información.
d. Proteger las copias de seguridad con el uso de mecanismos criptográficos cuando los requerimientos de confidencialidad así lo ameriten.

A.7. Política de transferencia de información.

Objetivo: definir las pautas generales para preservar la seguridad de la información que es transferida al interior y hacia el exterior de la Vicerrectoría de Investigaciones.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Diseñar e implementar procedimientos para proteger la información transferida contra intercepción, copiado, modificación, desviación y destrucción.
b. Implementar los controles necesarios para la protección de las instalaciones de comunicación**.**
c. Usar técnicas criptográficas para proteger la confidencialidad, integridad y disponibilidad de la información transferida por medio de mensajería electrónica. Ver la **política sobre el uso de la criptografía**[84].
d. Asesorar y concienciar al personal para que tome las debidas precauciones a fin de evitar la divulgación no autorizada de información confidencial.
e. Establecer acuerdos, con las partes externas, para la transferencia segura de información[85] que pueden llegar a incluir procedimientos para garantizar la trazabilidad y no repudiación; niveles aceptables de control de acceso; estándares técnicos para la transmisión de la información, etc.
f. Establecer procedimientos para proteger los medios físicos de transferencia de información contra el acceso no autorizado, hurto, mal uso o corrupción durante el transporte.

[84] Ver el Anexo A.2
[85] Como por ejemplo, los **acuerdos de confidencialidad**.

A.8. Política de protección contra malware

Objetivo: definir las pautas generales para garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra malware y software no deseado.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Implementar los controles necesarios para la detección, prevención y recuperación, a fin de proteger los activos de información contra malware y software no deseado. La VRI sostiene que siempre primará la prevención, pues la detección y recuperación no suelen ser el enfoque más adecuado.
b. Definir e implementar las reglas para la instalación de software.
c. Garantizar que la SI sea una parte integral de los sistemas de información a lo largo de todo el ciclo de vida de los mismos.
d. Reducir las vulnerabilidades que puedan ser explotadas por el malware mediante el desarrollo de la **política de gestión de vulnerabilidades técnicas[86].**
e. Incluir la **política de copias de respaldo[87]** en el diseño del plan de continuidad del negocio para la recuperación ante un ataque de malware.

A.9. Política de gestión de vulnerabilidades técnicas

Objetivo: definir las pautas generales para el diseño de un proceso de gestión a fin de prevenir la explotación de vulnerabilidades técnicas.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

[86] Ver Anexo A.9
[87] Ver Anexo A.6

a. Definir roles y responsabilidades para la gestión de vulnerabilidades técnicas[88].
b. Identificar los recursos que serán usados para la identificación de vulnerabilidades técnicas.
c. Obtener, de manera oportuna, información acerca de las vulnerabilidades técnicas de los sistemas de información vinculados al caso de estudio.
d. Evaluar el grado de exposición a las vulnerabilidades técnicas inherentes a los sistemas de información vinculados al caso de estudio.
e. Identificar, analizar y evaluar los riesgos de la SI asociados a las vulnerabilidades identificadas.
f. Definir e implementar los procedimientos y controles necesarios para reducir el riesgo asociado a las vulnerabilidades identificadas.
g. Mantener un registro de auditoría, alineado con **la política de registro y auditoría[89]**.
h. Monitorear y revisar, regularmente, el proceso de gestión de vulnerabilidades técnicas a fin de garantizar su efectividad y eficiencia.
i. Alinear el proceso de gestión de vulnerabilidades técnicas con las actividades de gestión de incidentes de la SI con el fin de facilitar la comunicación de las vulnerabilidades y la ejecución de los procedimientos de respuesta una vez ocurra un incidente.
j. Definir e implementar las reglas para la instalación de software para prevenir que se introduzcan nuevas vulnerabilidades que pueden afectar la confidencialidad, integridad y/o disponibilidad de los activos de información vinculados al caso de estudio.

A.10. Política sobre la responsabilidad de los activos

Objetivo: definir las pautas generales para identificar los activos de la Vicerrectoría de Investigaciones y definir las responsabilidades de protección necesarias.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

[88] Incluir el monitoreo, evaluación de riesgos de vulnerabilidades, instalación de parches, seguimiento de activos y cualquier otra responsabilidad que se requiera.
[89] Ver Anexo A.12

- Realizar y mantener un inventario de todos los activos de información y las instalaciones de procesamiento vinculadas al caso de estudio. La VRI garantizará que cada uno de estos activos tendrá asociado un responsable.
- Establecer un conjunto de reglas que permitan realizar un adecuado uso de los activos de información y de instalaciones de procesamiento vinculadas al caso de estudio.
- Obligar a cada empleado, vinculado al caso de estudio, a entregar los activos de información que estén bajo su responsabilidad cuando termine su contrato de trabajo.

A.11. Política de pantalla y escritorio limpio

Objetivo: definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Definir e implementar un procedimiento que protocolice el almacenamiento de información crítica en sitios seguros como una caja fuerte, gabinete y otros elementos o sitios.
b. Retirar, inmediatamente, los medios de comunicación que contengan información sensible, relacionada con la ejecución del caso de estudio.
c. Evitar el uso no autorizado de computadores, medios extraíbles, terminales, impresoras y demás dispositivos tecnológicos que contengan información relevante para el caso de estudio.
d. Requerir el uso de contraseñas para proteger el acceso a los dispositivos tecnológicos que contengan información relevante para el caso de estudio.
e. Obligar al personal a conservar su escritorio libre de información relacionada con el caso de estudio y que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
f. Obligar al personal a bloquear su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando, por cualquier motivo, deba abandonar su puesto de trabajo.

g. Obligar al personal a retirar, inmediatamente de la impresora, los documentos de carácter confidencial una vez estos son imprimidos. Se garantizará que estos no serán dejados en el escritorio sin custodia.
h. Rechazar el uso de fotocopiadoras, equipos de fax, cámaras digitales y, en general, cualquier equipo tecnológico que se encuentre desatendido.

A.12. Política de registro y auditoría

Objetivo: definir las pautas generales para mantener y proteger los registros de las transacciones electrónicas realizadas, de tal forma que sirvan como evidencia para los requerimientos de las auditorías (internas o externas) y como mecanismo para establecer responsabilidades de los usuarios, proveedores y administradores. De igual forma, establece los lineamientos para minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Producir, mantener y revisar los registros sobre las actividades de todos los usuarios[90], excepciones, fallos y demás eventos de la SI asociados al caso de estudio.
b. Garantizar que los administradores del sistema NO tengan permisos para borrar o desactivar los registros de sus actividades.
c. Proteger los registros contra la manipulación, eliminación y acceso no autorizado para evitar falsas sensaciones de seguridaA.
d. Sincronizar los relojes de todos los sistemas de procesamiento de información vinculados al caso de estudio para garantizar la precisión de los registros de auditoría, los cuales pueden ser requeridos en investigaciones o como evidencia en casos legales o disciplinarios.
e. Planear las actividades y requerimientos de las auditorías a sistemas operacionales vinculados al caso de estudio, con el fin de minimizar el impacto que puedan causar dichas actividades.
f. Limitar las auditorias con un acceso de "*solo lectura".*
g. Ejecutar fuera de las horas laborales todas las pruebas que puedan afectar la disponibilidad de los sistemas vinculados al caso de estudio.

[90]La palabra usuarios hace referencia tanto a los administradores como a los operadores del sistema.

A.13. Política para la seguridad en las redes de comunicaciones

Objetivo: definir las pautas generales para garantizar la protección de la información a su paso por las redes de comunicaciones e instalaciones de procesamiento.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Gestionar y controlar las redes de comunicaciones para proteger la información, vinculada al caso de estudio, que es almacenada y procesada por aplicativos informáticos.
b. Proteger la privacidad y confidencialidad de la información transmitida a través de redes públicas y/o redes privadas que, estando al interior del edificio de la VRI, intervienen en la ejecución del caso de estudio. Para ello, se acudirá a la **política del uso de la criptografía**[91] y a **la política de transferencia de información**[92].
c. Registrar y monitorear los eventos de los servicios de reA.
d. Segregar los grupos de servicios, usuarios y sistemas de información vinculados al caso de estudio, separándolos en dominios distintos con sus respectivos perímetros bien definidos (por ejemplo: dominios de acceso público, dominio de servidores, redes inalámbricas, etc.).
e. Coordinar actividades de gestión para optimizar los servicios de red y garantizar que los controles estén completamente implementados a lo largo de toda la infraestructura de red que, estando al interior del edificio de la VRI, interviene en la ejecución del caso de estudio.
f. Restringir la conexión y acceso a la red por parte de sistemas y entes terceros.
g. Incluir, en los acuerdos con los proveedores de los servicios de red, los mecanismos de seguridad y los niveles de servicio requeridos para el desarrollo de las actividades del caso de estudio.

[91] Ver Anexo A.2
[92] Ver Anexo A.7

A.14. Política para la adquisición, desarrollo y mantenimiento de sistemas

Objetivo: definir las pautas generales para garantizar que la SI sea una parte integral de los sistemas de información durante todo el ciclo de vida de los mismos.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Establecer y aplicar reglas para el desarrollo de software.
b. Establecer, documentar y mantener principios para la construcción de sistemas seguros.
c. Incluir los requisitos de la SI en el desarrollo y mantenimiento de los sistemas de información.
d. Proteger la información involucrada en las transacciones de los servicios de las aplicaciones vinculadas al caso de estudio, con el fin de evitar la transmisión incompleta, el enrutamiento errado y la alteración, divulgación, duplicación o reproducción no autorizada de los mensajes.
e. Controlar los cambios a los sistemas de información y paquetes de software mediante el uso de procedimientos formales de control de cambios.
f. Establecer y proteger adecuadamente los ambientes de desarrollo seguro.
g. Realizar pruebas de funcionalidad de la seguridad durante el desarrollo de los sistemas de información vinculados al caso de estudio.
h. Seleccionar, proteger y controlar, cuidadosamente, los datos de prueba usados durante el desarrollo de los sistemas vinculados al caso de estudio.

A.15. Política para el cumplimiento de requisitos legales y contractuales

Objetivo: definir las pautas generales para evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la SI en la Vicerrectoría de Investigaciones.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Identificar y documentar las obligaciones legales, estatutarias, reglamentarias y contractuales pertinentes.
b. Cumplir con las obligaciones legales, estatutarias, reglamentarias y contractuales pertinentes que se encuentran relacionadas con patentes y derechos de propiedad intelectual.
c. Aplicar la **política del uso de la criptografía**[93] a fin de dar cumplimiento a la ley 527 de 1999 [35] y demás normas asociadas.

A.16. Política para la continuidad de la SI

Objetivo: definir las pautas generales para garantizar que la SI sea incluida en los planes de gestión de la continuidad del negocio de la Vicerrectoría de Investigaciones.

Directrices: la VRI, en aras de proteger sus activos de información, vinculados al caso de estudio, y contribuir a la implementación y certificación del SGSI de la Universidad del Cauca, ha decidido:

a. Determinar, de forma clara, los requisitos frente a la continuidad de la SI en el caso de estudio.
b. Asegurar el nivel de continuidad requerido para enfrentar las situaciones adversas mediante el establecimiento, documentación, implementación y mantenimiento de procesos, procedimientos y controles.
c. Dotar a las instalaciones de procesamiento de información con la suficiente redundancia a fin de garantizar la disponibilidad del servicio.

[93] Ver Anexo A.2

Anexo B

Plantilla genérica de seguridad (GST)

Esta guía tiene por objetivo proponer el diseño de las plantillas genéricas de seguridad como un mecanismo para reportar y comunicar los incidentes de SI en el caso de estudio, generando conocimiento de manera colaborativa entre el personal. Gracias a ello, además de reportar los incidentes, también se evitará la reaparición de los mismos mediante el aprendizaje obtenido a partir de los errores cometidos.

A continuación, en la Tabla B1, se expone la plantilla propuesta para el reporte de incidentes de la SI en el caso de estudio, la cual es obtenida a partir de la adaptación de los aportes hechos por [57] y [58]. Esta plantilla deberá ser diligenciada describiendo el evento con la mayor precisión y objetividad posible. Una vez diligenciada la plantilla, ésta deberá ser reportada al CISO[94] tal y como lo establece la estructura organizacional propuesta por la sección 3.1.6 en la Tabla 3.1.

Fecha de notificación:	Hora de notificación:
Datos de la persona que reporta el incidente	
Apellidos y Nombres:	
Sede(Principal, Santander, Miranda) donde trabaja o estudia:	Área/Dependencia/Facultad a la que pertenece:
Teléfono Celular:	Número de Oficina (para funcionarios y profesores):
Teléfono fijo y Extensión (para funcionarios y profesores):	

[94] Oficial de la SI

Correo Electrónico:
Información sobre el incidente
Fecha en que se observó el incidente: / Hora en que se observó el incidente:
Marque con una **X** todas las opciones que considere aplicable: ◯ Uso indebido de los activos de información ◯ Uso inadecuado de un recurso informático o red de la Universidad del Cauca ◯ Divulgación no autorizada de información personal ◯ Intrusión física en alguna de las instalaciones universitarias ◯ Robo, pérdida o destrucción no autorizada de un activo de Información ◯ Interrupción en un sistema o servicio de red ◯ Modificación, Instalación o eliminación no autorizada de software de gestión de información ◯ Acceso o intento de acceso no autorizado a uno o varios sistemas de gestión de información ◯ Acceso o intento de acceso no autorizado a uno o varios activos de Información de la institución ◯ Ingeniería social, fraude o phishing ◯ Modificación no autorizada de un sitio o página web de la Universidad. ◯ Eliminación insegura de información. ◯ Modificación o eliminación no autorizada de datos. ◯ Anomalía o vulnerabilidad técnica de software. ◯ Amenaza o acoso por medio electrónico. ◯ Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.) ◯ Robo o pérdida de un recurso informático de la Universidad. ◯ Daño a causa de origen natural ◯ Daño a causa de una mala manipulación de los activos de información ◯ Degradación de soportes de almacenamiento de información ◯ Error de usuario ◯ Error de administrador ◯ Vulnerabilidad de un programa software ◯ Otro. ¿Cual?:
Describa el incidente:

<table>
<tr><td colspan="2">Describa de forma clara y concisa como detectó el incidente:</td></tr>
<tr><td>¿El incidente está en progreso? (Marque con una X):

[ ] SI [ ] NO</td><td>Tiempo que duró el incidente:

Nota: En caso de que el incidente aún se encuentre en progreso, especifique el tiempo estimado de la duración de este</td></tr>
<tr><td>Activo comprometido (Documento, Dispositivo, Personal y otros):</td><td>Nombre de la persona propietaria del activo:</td></tr>
<tr><td colspan="2">Seleccione con una X el (los) tipo (s) de conexión que tiene el o los equipos que presentaron el incidente:

◯ Conexión a Internet
◯ Conexión a la red de la Universidad del Cauca
◯ ninguna</td></tr>
<tr><td colspan="2">Usuarios afectados por el incidente:

[ ] NO APLICA</td></tr>
<tr><td colspan="2">Personas que intervinieron de alguna forma en el incidente:

……
……
……
……
……
……</td></tr>
<tr><td colspan="2">¿Existe una copia de respaldo de la información afectada?

[ ] SI [ ] NO [ ] NO APLICA</td></tr>
</table>

Tabla B.1. Formato de Reporte de Incidentes de la SI

Anexo C

Resultados de la gestión del riesgo

A continuación se exponen los resultados obtenidos de ejecutar la cuarta fase del proceso de planeación de un SGSI mediante la aplicación del MARA, logrando satisfacer los siguientes entregables requeridos por dicha fase:

- *Reportes de la valoración del riesgo.*
- *Lista de controles y objetivos de control seleccionados.*
- *Plan de tratamiento de riesgos (PTR).*
- *Aprobación de la implementación del SGSI.*
- *Aceptación de los riesgos residuales.*
- *Declaración de Aplicabilidad (SOA)*

C.1. Resultados de la caracterización de los activos

C.1.1. Dependencias entre los activos

A continuación, la Tabla C.1 expone en detalle las dependencias existentes entre los activos de información vinculados al caso de estudio, los cuales se encuentran agrupados por capas de acuerdo a la distribución expuesta por la Tabla 6.1[95]. En la Tabla C.1, en la columna:

- ***ID activo superior*** se hace referencia a un identificador temporal para los activos.
- **ID activo inferior** se listan los activos de los cuales depende un activo en particular.

[95] Cabe recordar que esto fue necesario para poder aprovechar la ayuda que suministra PILAR para la determinación de las dependencias.

CAPA	ID activo superior	Activo superior	Dependencias con activos inferiores			
			ID activo inferior	Grado de dependencia (%)		
				C	D	I
Activos Esenciales	1	Información	4	100	50	90
			5	100	50	10
			6	100	-	25
	2	Servicio de secretaría de la VRI	4	-	50	-
			5	-	50	-
			6	-	10	-
			8	-	50	-
			9	-	25	-
			10	-	100	-
			12	-	50	-
	3	Servicio de Apoyo al Investigador	4	-	50	-
			5	-	50	-
			6	-	10	-
			8	-	50	-
			9	-	25	-
			10	-	100	-
			12	-	50	-
Sistema Información	4	SIVRI (Sistema de Información de la VRI)	7	100	100	100
			8	100	-	100
			9	100	-	1
			11	100	100	100
Soportes información	5	Documentos físicos	10	100	-	100
			12	100	100	100
	6	Dispositivos de almacenamiento de información digital.	8	100	-	100
			10	100	-	100
Equipos informáticos	7	Servidores	10	100	-	100
			11	100	75	100
			13	-	50	-
			14	-	50	-
			16	100	100	100

	8	Computadores personales.	10	100	-	100
			11	100	-	75
			14	-	50	-
			15	100	100	100
	9	Fotocopiadora Multifuncional	10	100	-	100
			11	100	75	75
			14	-	50	-
			15	100	100	100
Personal	10	Personal	15	100	100	100
Redes	11	Redes de área local (LAN y WLAN)	10	100	10	100
			15	100	100	100
			16	100	100	100
Equipos auxiliares	12	Satélite	17	100	100	100
	13	Equipos de Climatización	16	-	100	-
	14	UPS	15	-	100	-
			16	-	100	-
Instalaciones	15	Oficinas del personal	-	-	-	-
	16	Cuarto de servidores	-	-	-	-
	17	Almacén Archivo Satélite VRI	-	-	-	-

Tabla C.1. Dependencias entre los activos

C.1.2. Resultados de la valoración de los activos.

Con el apoyo de PILAR, cargada con los criterios propuestos por el Anexo A.3.1 y considerando la escala ilustrada por la Tabla 5.21, los resultados de las tareas previas y la guía suministrada por la sección 5.3.3, se logró valorar las 3 dimensiones

primarias de los activos esenciales con ayuda del propietario de los mismos[96], obteniendo los resultados que se ilustran, a continuación, por la Tabla C.2.

Nombre del activo	Criterios cumplidos	Tipo	Valor		
			C	D	I
Presupuesto global de cada proyecto de investigación	Confidencialidad: 8.ci,7.ip, 7.rep.a, 9.ic.c, 9.ic.d, 7.ic.d Disponibilidad: 7.iap.a, 6.trs Integridad: 7.ip, 9.ic.d	Información pública clasificada	9	7	9
Avales concedidos a cada proyecto de investigación.	Confidencialidad: 10.ci Disponibilidad: 7.iap.a, 9.rep.b, 9.ope, 9.trs Integridad: 10.s.a, 10.s.b, 9.rep.a, 9.rep.b, 9.ic.c, 9.ic.d	Información pública reservada	10	9	10
Actas de reunión del Consejo de Investigaciones y del Comité de Ética.	Confidencialidad: 8.ci Disponibilidad: 7.s.b, 5.iap.a, 5.iap.b, 5.ope Integridad: 10.s.a, 10.s.b, 9.rep, 9.ic.d, 5.ope	Información pública clasificada	8	7	10
Convenios - Contratos con entidades financiadoras	Confidencialidad:10.ci, Disponibilidad: 10.s.b, 9.ic.d, 9.trs Integridad: 10.s.a, 10.s.b, 9.rep.a, 9.rep.b, 9.ic.b, 9.ic.c, 9.ic.d	Información pública reservada	10	10	10
Documentos de viabilidad financiera de los proyectos de investigación.	Confidencialidad:10.ci Disponibilidad: 9.s.b, 7.iap.a, 7.ope, 6.trs Integridad: 9.s.a, 9.s.b, 9.rep.a, 9.rep.b, 9.ic.c	Información pública reservada	10	9	9

[96] El jefe de la División de Gestión de Investigación, responsable de la ejecución del caso de estudio.

Oficios remisorios a las entidades externas financiadoras.	Confidencialidad: 8.ci Disponibilidad: 9.s.b, 7.rep.a, 7.rep.b, 9.ic.d, 7.ic.d Integridad: 9.s.a, 9.s.b, 9.rep.a, 9.rep.b, 9.ic.c, 9.ic.d	Información pública clasificada	9	6	9
Oficios remisorios a la División de Gestión Financiera.	Confidencialidad: 8.ci, 7.s.b, 7.rep.b, 7.ic.c Disponibilidad: 3.iap.a, 3.trs Integridad: 7.s.a, 7.s.b, 7.rep.b, 7.ic.c	Información pública clasificada	8	3	7
Informes financieros sobre la ejecución presupuestal de los proyectos de investigación.	Confidencialidad: 10.ci Disponibilidad: 9.s.b, 9.iap.a, 7.ope, 9.trs Integridad: 9.s.a, 9.s.b, 9.rep.a, 9.rep.b, 9.ic.b, 9.ic.c, 9.ic.d, 7.ope	Información pública reservada	10	9	9
Informes técnicos, parciales o finales, de los proyectos de investigación.	Confidencialidad: 8.ci, 7.iap.a, 5.rep.a, 7.ic.c, 7.ope Disponibilidad: 5.s.b, 7.iap.a, 7.rep.a, 7.rep.b, 7.ic.d, 7.ope, 6.trs Integridad: 9.s.b, 9.rep.a, 9.rep.b, 9.ic.c, 9.ic.d	Información pública clasificada	8	7	9
Actas de Liquidación de convenios-contratos con entidades externas.	Confidencialidad: 2.ci Disponibilidad: 7.s.b, 7.ic.c, 6.trs Integridad: 9.s.a, 9.rep.a, 9.rep.b, 9.ic.b, 9.ic.c	Información pública	2	7	9
Certificados de Disponibilidad Presupuestal (CDP)	Confidencialidad: 10.ci Disponibilidad: 9.s.b, 7.iap.a, 7.rep.a, 7.rep.b, 9.ic.c, 9.ic.d, 10.ope, 9.trs Integridad: 9.s.a, 9.s.b, 9.rep.b, 9.ic.b, 9.ic.c	Información pública reservada	10	10	9

Ordenes de Prestación de Servicios (OPS)	Confidencialidad: 10.ci Disponibilidad: 7.iap.a, 7.rep.b, 7.ope, 9.trs Integridad: 9.s.a, 9.s.b, 9.rep.b, 9.ic.b, 9.ic.c	Información pública reservada	10	9	9
Solicitud de avance para compras o comisión de servicios	Confidencialidad: 8.ci Disponibilidad: 7.iap.a, 7.rep.b, 9.ope, 9.trs Integridad: 7.s.a, 7.rep.b, 7.ic.b, 7.ic.c	Información pública reservada	8	9	7
Orden de suministros	Confidencialidad: 10.ci Disponibilidad: 5.iap.a, 7.rep.b, 7.ope, 6.trs Integridad: 7.s.a, 7.rep.b, 7.ic.b, 7.ic.c	Información pública reservada	10	7	7
Registros de Disponibilidad Presupuestal	Confidencialidad: 10.ci Disponibilidad: 10.s.b, 5.iap.a, 7.rep.b, 9.trs Integridad: 9.rep.b, 9.ic.b, 9.ic.c	Información pública reservada	10	10	9
Órdenes de Pago	Confidencialidad: 10.ci Disponibilidad: 10.s.b, 7.iap.a, 7.rep.b, 9.ope, 9.trs Integridad: 10.s.a, 10.s.b, 9.rep.a, 9.rep.b, 9.ic.b, 9.ic.c, 9.ic.d	Información pública reservada	10	10	10
Servicio de secretaría	Confidencialidad: No aplica Disponibilidad: 9.iap.a, 9.rep.b, 9.ope, 9.trs Integridad: No aplica	Servicios	0	9	0
Servicio de apoyo al Investigador	Confidencialidad: No aplica Disponibilidad: 9.iap.a, 9.rep.b, 9.ope, 9.trs Integridad: No aplica	Servicios	0	9	0

Tabla C.2. Valor de los activos esenciales

Luego, los activos restantes heredaron el valor de los activos esenciales de acuerdo al grado de dependencia que existía entre éstos. De esta manera, se obtuvo los resultados expuestos por la Tabla C.3.

Capa	Nombre del activo	Tipo	Valor		
			C	D	I
Sistemas de Información	SIVRI	Software	10	9	10
Soportes de información	Documentos físicos	Soportes de información	10	9	7
	Dispositivos de almacenamiento de información digital.	Soportes de información	10	6	8
Personal	Personal vinculado al caso de estudio.	Personal	10	9	10
Equipos Informáticos	Servidores	Combinación de software y hardware	10	9	10
	Computadores personales.	Combinación de software y hardware	10	8	10
	Fotocopiadoras Multifuncionales	Hardware	8	7	0
Redes	Redes de Área Local (LAN y WLAN)	Redes de comunicación	10	10	10
Equipos Auxiliares	Satélite (Sistema de Archivo)	Equipamiento auxiliar	10	9	10
	Equipos de Climatización	Equipamiento auxiliar	0	8	0
	UPS	Equipamiento auxiliar	0	8	0
Instalaciones	Oficinas del personal	Instalaciones	10	10	10
	Cuarto de servidores	Instalaciones	10	10	10
	Almacén Archivo Satélite VRI	Instalaciones	10	9	10

Tabla C.3. Valor de los activos no esenciales

C.2. Resultados de la caracterización de las amenazas

Considerando el *Modelo de valor*[97]*,* los datos estándar suministrados por PILAR, la guía, escalas y criterios definidos por la sección 5.3.4 y lo discutido por la sección 6.1.2, se logró:

- Identificar las amenazas que atentan contra los activos de información vinculados al caso de estudio, satisfaciendo el producto de salida: *Relación de amenazas posibles,* requerido por la tarea MARA 2.1.

- Determinar la probabilidad de ocurrencia de las amenazas y la degradación que éstas causan sobre el valor de los activos, satisfaciendo el producto de salida: *Mapa de riesgos,* requerido por la tarea MARA 2.2.

A continuación, la Tabla C.4 expone los resultados mencionados anteriormente mostrando la degradación en cada una de las dimensiones primarias: Confidencialidad (C), Disponibilidad (D) e Integridad (I).

Escala para la degradación				
Muy Alta	Alta	Media	Baja	Despreciable
Escala para la probabilidad				
Casi seguro	Muy alta	Posible	Poco probable	Muy rara

C: Confidencialidad D:Disponibilidad I: Integridad

Activo	**Amenaza**	**Probabilidad**	**Degradación**		
			C	**D**	**I**
Personal	Enfermedad	P	0%	100%	0%
	Huelga	PP	0%	100%	0%
	Extorsion	P	100%	1%	100%
	Ingeniería social (picaresca)	MA	100%	1%	100%
SIVRI	Avería de origen físico o lógico	MA	0%	50%	0%
	Errores de los Usuarios	MA	10%	1%	10%
	Errores del administrador del sistema	P	20%	20%	20%
	Alteración de la información	P	0%	0%	25%
	Fugas de la información	MA	10%	0%	0%
	Vulnerabilidades de los programas (software)	MA	20%	1%	20%
	Suplantación de la identidad	CS	50%	0%	50%

[97] Obtenido en la sección 6.1.1 por la tarea MARA 1.3

	Abuso de privilegios de acceso	MA	10%	1%	10%
	Uso no previsto	P	10%	1%	10%
	Acceso no autorizado	CS	60%	0%	10%
	Repudio (negación de actuaciones)	P	0%	0%	100%
	Modificación de la información	MA	0%	0%	50%
	Destrucción de la información	P	0%	100%	0%
	Revelación de la información	MA	100%	0%	0%
	Manipulación de programas	P	100%	50%	100%
Documentos físicos	Fuego	MR	0%	100%	0%
	Daños por agua	MA	0%	100%	0%
	Condiciones inadecuadas de temperatura o humedad	CS	0%	25%	0%
	Errores de los usuarios	MA	10%	1%	5%
	Suplantación de la identidad	CS	50%	0%	0%
	Acceso no autorizado	MA	100%	25%	0%
	Destrucción información	MA	0%	100%	0%
	Robo de documentos	P	100%	100%	0%
	Revelación de la información	MA	100%	0%	0%
Dispositivos de almacenamiento digital	Fuego	MR	0%	100%	0%
	Daños por agua	PP	0%	100%	0%
	Contaminación electromagnética	MR	0%	25%	0%
	Avería de origen físico o lógico	P	0%	50%	0%
	Degradación de los soportes de almacenamiento	P	0%	100%	0%
	Errores de los usuarios	MA	50%	25%	25%
	Errores de mantenimiento / actualización de equipo (hardware)	PP	0%	100%	0%
	Pérdida de equipos	PP	100%	10%	0%
	Uso no previsto	MA	1%	1%	10%
	Acceso no autorizado	MA	100%	25%	100%
	Repudio	P	0%	0%	100%
	Modificación de la información	P	0%	0%	100%
	Revelación de la información	MR	100%	0%	0%
	Manipulación de hardware	PP	50%	0%	50%
	Robo de equipos	P	100%	25%	0%
Servidores (Soporte SVRI)	Avería de origen físico y lógico	P	0%	50%	0%
	Corte del suministro eléctrico	MA	0%	100%	0%
	Condiciones inadecuadas de temperatura o humedad	P	0%	100%	0%
	Errores del administrador del sistema	P	20%	20%	20%

	Errores de monitorización (log)	MA	100%	0%	10%
	Errores de configuración	MA	100%	0%	10%
	Difusión de software dañino	P	10%	10%	10%
	Fugas de información	P	25%	0%	0%
	Vulnerabilidades de los programas (software)	P	20%	10%	20%
	Errores de mantenimiento / actualización de equipos (hardware)	P	0%	10%	0%
	Caída del sistema por agotamiento de recursos	P	0%	50%	0%
	Manipulación de los registros de actividad (log)	MA	0%	0%	50%
	Manipulación de los ficheros de configuración	MA	25%	10%	25%
	Suplantación de la identidad	MA	50%	0%	50%
	Abuso de privilegios de acceso	P	100%	10%	100%
	Uso no previsto	P	100%	10%	10%
	Difusión de software dañino	PP	100%	100%	100%
	Acceso no autorizado	MA	100%	10%	100%
	Repudio (negación de actuaciones)	P	0%	0%	100%
	Modificación de la información	P	0%	0%	50%
	Destrucción de la información	P	0%	25%	0%
	Revelación de la información	MA	50%	0%	0%
	Manipulación de programas	P	100%	50%	100%
	Manipulación del hardware	PP	50%	50%	0%
	Ataque destructivo	PP	0%	100%	0%
	Denegación de servicio	MA	0%	100%	0%
	Robo de equipos	MR	100%	100%	0%
Satélite (Sistema de archivo)	Errores de los usuarios	MA	10%	10%	10%
	Modificación de la información	MA	0%	0%	100%
	Destrucción de la información	MA	0%	100%	0%
	Revelación de la información	MA	100%	0%	0%
	Ataque destructivo	PP	0%	75%	0%
Almacenes Satélite	Fuego	MR	0%	100%	0%
	Terremotos	MR	0%	100%	0%
	Daños por agua	MA	0%	100%	0%
	Contaminación medioambiental	P	0%	10%	0%
	Uso no previsto	CS	50%	10%	10%
	Acceso no autorizado	CS	50%	0%	10%
	Ataque destructivo	MR	0%	100%	0%
	Avería de origen físico y lógico	P	0%	50%	0%

Redes de área local (LAN Y WLAN)	Corte del suministro eléctrico	MA	0%	100%	0%
	Fallo de servicios de comunicaciones	P	0%	50%	0%
	Errores del administrador del sistema	P	20%	20%	20%
	Errores de [re-]encadenamiento	P	10%	0%	0%
	Errores de secuencia	P	0%	0%	10%
	Errores de mantenimiento / actualización de equipos (hardware)	P	0%	10%	0%
	Uso no previsto	MA	10%	75%	10%
	[Re-]encadenamiento de mensajes	P	10%	0%	0%
	Alteración de secuencia	P	0%	0%	10%
	Acceso no autorizado	CS	75%	10%	10%
	Análisis de tráfico	MA	2%	0%	0%
	Interceptación de información (escucha)	MA	5%	0%	0%
	Manipulación de hardware	P	50%	100%	0%
	Denegación de servicio	CS	0%	90%	0%
	Robo de equipos	PP	10%	75%	0%
	Ataque destructivo	PP	0%	100%	0%
Cuarto de servidores	Fuego	MR	0%	100%	0%
	Terremotos	MR	0%	100%	0%
	Daños por agua	MR	0%	100%	0%
	Contaminación medioambiental	P	0%	10%	0%
	Contaminación electromagnética	PP	0%	10%	0%
	Uso no previsto	CS	50%	10%	10%
	Acceso no autorizado	CS	50%	0%	10%
	Ataque destructivo	MR	0%	100%	0%
Computadores personales	Avería de origen físico y lógico	P	0%	50%	0%
	Corte del suministro eléctrico	MA	0%	100%	0%
	Condiciones inadecuadas de temperatura o humedad	P	0%	100%	0%
	Errores de los usuarios	MA	25%	10%	10%
	Errores de monitorización (log)	MA	0%	0%	1%
	Errores de configuración	MA	0%	0%	1%
	Fugas de información	CS	10%	0%	0%
	Vulnerabilidades de los programas (software)	MA	20%	1%	20%
	Errores de mantenimiento / actualización de programas (software)	MA	0%	1%	1%

	Errores de mantenimiento / actualización de equipos (hardware)	MA	0%	25%	0%
	Manipulación de los registros de actividad (log)	MA	0%	0%	50%
	Manipulación de los ficheros de configuración	MA	10%	10%	10%
	Suplantación de la identidad	MA	50%	0%	50%
	Abuso de privilegios de acceso	MA	100%	10%	100%
	Uso no previsto	MA	100%	10%	10%
	Difusión de software dañino (propagación intencionada de virus, espías, gusanos, troyanos, bombas lógicas, etc.)	MA	100%	100%	100%
	Acceso no autorizado	MA	100%	10%	100%
	Repudio (negación de actuaciones)	P	0%	0%	100%
	Modificación de la información	MA	0%	0%	50%
	Destrucción de la información	MA	0%	25%	0%
	Revelación de la información	MA	50%	0%	0%
	Manipulación de programas	MA	100%	50%	100%
	Manipulación del hardware	P	50%	75%	0%
	Ataque destructivo	PP	0%	100%	0%
	Denegación de servicio	MA	0%	100%	0%
	Robo de equipos	P	0%	100%	0%
Oficinas del personal	Fuego	MR	0%	100%	0%
	Terremotos	MR	0%	100%	0%
	Daños por agua	MA	0%	100%	0%
	Contaminación medioambiental	P	0%	10%	0%
	Contaminación electromagnética	PP	0%	10%	0%
	Uso no previsto	CS	50%	10%	10%
	Acceso no autorizado	CS	50%	0%	10%
	Ataque destructivo	MR	0%	100%	0%
Fotocopiadoras multifuncionales	Avería de origen físico y lógico	P	0%	75%	0%
	Corte del suministro eléctrico	MA	0%	100%	0%
	Condiciones inadecuadas de temperatura o humedad	P	0%	100%	0%
	Errores de mantenimiento / actualización de equipos (hardware)	MA	0%	10%	0%
	Uso no previsto	MA	100%	75%	100%
	Acceso no autorizado	CS	100%	25%	100%
	Revelación de la información	MA	50%	0%	0%

	Ataque destructivo	PP	0%	100%	0%
	Manipulación del hardware	P	50%	50%	0%
	Denegación de servicio	MA	0%	100%	0%
	Robo de equipos	MR	100%	100%	0%
Equipos de climatización	Corte del suministro eléctrico	MA	0%	100%	0%
	Errores del mantenimiento / actualización de equipos (hardware)	P	0%	75%	0%
	Uso no previsto	MA	0%	50%	0%
	Robo de equipos	PP	0%	100%	0%
	Ataque destructivo	PP	0%	75%	0%
Fuentes de Alimentación Ininterrumpida	Errores de mantenimiento / actualización de equipos (hardware)	P	0%	25%	0%
	Uso no previsto	MA	0%	50%	0%
	Manipulación de hardware	P	0%	25%	0%
	Robo de equipos	PP	0%	100%	0%
	Ataque destructivo	MR	0%	100%	0%

Tabla C.4. Resultados de la valoración de las amenazas

Cabe mencionar que se consideró totalmente innecesario intentar identificar las amenazas que puedan atentar sobre los activos esenciales, esto debido a que la metodología MAGERIT V3 en [22] afirma que las amenazas no suelen materializarse sobre los activos esenciales sino, más bien, sobre los activos que los soportan. Para mayor información, retomar la sección 6.1.2.

C.3. Resultados de la estimación del riesgo

Como se discutió en la sección 6.1.3, en el caso de estudio no se han diseñado ni implementado formalmente los controles para proteger los activos de información, evidenciando una desatención generalizada por la SI y un desconocimiento total de los controles que la norma ISO/IEC 27001 [2] sugiere en su Anexo A.

Considerando lo discutido anteriormente, el *Modelo de valor*[98] y el *Mapa de riesgos*[99], se logró determinar el impacto potencial al que se encuentran sometidos los activos de información vinculados al caso de estudio, lo cual es evidenciado por la Tabla C.5.

[98] Informe de valor de los activos. Obtenido en la sección 6.1.1 por la tarea MARA 1.3
[99] Informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos. Obtenido en la sección 6.1.2 por la tarea MARA 2.2

De esta manera se logró satisfacer el producto de salida: *informe de impacto potencial,* requerido por la tarea MAR 3.1.

Luego, al ejecutar la tarea MAR 3.2, se consiguió estimar el riesgo asociado a cada amenaza identificada y, a la vez, fue posible identificar las prioridades de tratamiento, como lo evidencia, a continuación, la Tabla C.5[100]. De esta manera se logró satisfacer el producto de salida: *informe de riesgo potencial,* requerido por la tarea MARA 3.2. Lo anterior fue obtenido con base en:

- El *Modelo de valor*
- El *Mapa de riesgos*
- El *Informe de impacto potencial*[101]
- La escala del nivel de riesgo ilustrada por la Tabla 5.30
- Las directrices definidas por la sección 5.3.5 para el cálculo del valor ponderado del riesgo
- Los criterios para la evaluación de riesgos propuestos en la sección 5.3.5 para establecer las prioridades de tratamiento.

Escala para el nivel de riesgo				
Crítico	Alto	Medio	Bajo	Despreciable

C=Confidencialidad I=Integridad D=Disponibilidad P=Ponderado

ID	Amenaza	Activo	Impacto			Riesgo			
			C	D	I	C	D	I	P
RIESGOS DE ALTA PRIORIDAD									
R1	Ingeniería social (picaresca)	Personal	10	0,1	10	8	0,1	8	5,6
R2	Acceso no autorizado	Dispositivos de almacenamiento digital	10	1,5	8	8	1,2	6,4	5,5
R8	Manipulación de programas	SIVRI	10	4,5	10	5	2,3	5	4,2
R3	Acceso no autorizado	Documentos físicos	10	2,3	0	8	1,8	0	3,7
R9	Extorsión	Personal	10	0,1	10	5	0	5	3,5
R10	Suplantación de la identidad	SIVRI	5	0	5	5	0	5	3,5
R11	Robo de documentos	Documentos físicos	10	9	0	5	4,5	0	3,4

[100] Cabe mencionar que, de acuerdo con los criterios propuestos por la sección 5.7 en la Tabla 5.12, los riesgos con un valor ponderado *Despreciable,* serán excluidos de la Tabla C.5.
[101] Obtenido por la tarea MARA 3.1 en la sección 6.1.3

R4	Revelación de la información	SIVRI	10	0	0	8	0	0	3,2
R5	Revelación de la información	Documentos físicos	10	0	0	8	0	0	3,2
R7	Acceso no autorizado	SIVRI	6	0	1	6	0	1	2,7
R18	Errores de los usuarios	Dispositivos de almacenamiento digital	5	1,5	2	4	1,2	1,6	2,4
R12	Robo de equipos	Dispositivos de almacenamiento digital	10	1,5	0	5	0,8	0	2,2
R6	Destrucción información	Documentos físicos	0	9	0	0	7,2	0	2,2
R14	Suplantación de la identidad	Documentos físicos	5	0	0	5	0	0	2
R13	Repudio (negación de actuaciones)	SIVRI	0	0	10	0	0	5	1,5
R16	Destrucción Intencional de la información	SIVRI	0	9	0	0	4,5	0	1,4
R24	Pérdida de equipos	Dispositivos de almacenamiento digital	10	0,6	0	3	0,2	0	1,3
R19	Modificación Intencionada de la información	SIVRI	0	0	5	0	0	4	1,2
R20	Repudio	Dispositivos de almacenamiento digital	0	0	8	0	0	4	1,2
R21	Modificación de la información	Dispositivos de almacenamiento digital	0	0	8	0	0	4	1,2
RIESGOS DE PRIORIDAD MEDIA									
R34	Acceso no autorizado	Servidores	10	0,9	10	8	0,7	8	5,8
R43	Manipulación de programas	Servidores	10	4,5	10	5	2,3	5	4,2
R44	Abuso de privilegios de acceso	Servidores	10	0,9	10	5	0,5	5	3,6
R38	Acceso no autorizado	Redes de área local	7,5	1	1	7,5	1	1	3,6
R60	Difusión de software dañino	Servidores	10	9	10	3	2,7	3	2,9
R53	Suplantación de la identidad	Servidores	5	0	5	4	0	4	2,8

R33	Denegación de servicio	Redes de área local	0	9	0	0	9	0	2,7
R45	Uso no previsto	Cuarto de servidores	5	1	1	5	1	1	2,6
R46	Uso no previsto	Almacenes Satélite	5	0,9	1	5	0,9	1	2,6
R51	Manipulación de hardware	Redes de área local	5	10	0	2,5	5	0	2,5
R36	Modificación Intencionada de la información	Satélite	0	0	10	0	0	8	2,4
R37	Corte del suministro eléctrico	Redes de área local	0	10	0	0	8	0	2,4
R42	Uso no previsto	Redes de área local	1	7,5	1	0,8	6	0,8	2,4
R47	Acceso no autorizado	Almacenes Satélite	5	0	1	5	0	1	2,3
R48	Acceso no autorizado	Cuarto de servidores	5	0	1	5	0	1	2,3
R49	Uso no previsto	Servidores	10	0,9	1	5	0,5	0,5	2,3
R39	Corte del suministro eléctrico	Servidores	0	9	0	0	7,2	0	2,2
R40	Denegación de servicio	Servidores	0	9	0	0	7,2	0	2,2
R41	Destrucción Intencionada de la información	Satélite	0	9	0	0	7,2	0	2,2
R64	Daños por agua	Almacenes Satélite	0	9	0	0	7,2	0	2,2
R72	Manipulación de los ficheros de configuración	Servidores	2,5	0,9	2,5	2	0,7	2	1,6
R58	Revelación de la información	Servidores	5	0	0	4	0	0	1,6
R50	Repudio	Servidores	0	0	10	0	0	5	1,5
R52	Condiciones inadecuadas de temperatura o humedad	Servidores	0	9	0	0	4,5	0	1,4
R59	Manipulación de los registros de actividad (log)	Servidores	0	0	5	0	0	4	1,2
RIESGOS DE PRIORIDAD BAJA									

R79	Difusión de software dañino	Computadores personales	10	8	10	8	6,4	8	7,5
R80	Manipulación de programas	Computadores personales	10	4	10	8	3,2	8	6,6
R78	Acceso no autorizado	Computadores personales	10	0,8	10	8	0,6	8	5,8
R81	Abuso de privilegios de acceso	Computadores personales	10	0,8	10	8	0,6	8	5,8
R84	Uso no previsto	Fotocopiadoras multifuncionales	8	5,3	0	6,4	4,2	0	3,8
R83	Acceso no autorizado	Fotocopiadoras multifuncionales	8	1,8	0	8	1,8	0	3,7
R82	Uso no previsto	Computadores personales	10	0,8	1	8	0,6	0,8	3,6
R93	Suplantación de la identidad	Computadores personales	5	0	5	4	0	4	2,8
R90	Uso no previsto	Oficinas del personal	5	1	1	5	1	1	2,6
R106	Daños por agua	Oficinas del personal	0	10	0	0	8	0	2,4
R91	Acceso no autorizado	Oficinas del personal	5	0	1	5	0	1	2,3
R85	Corte del suministro eléctrico	Computadores personales	0	8	0	0	6,4	0	1,9
R86	Denegación de servicio	Computadores personales	0	8	0	0	6,4	0	1,9
R87	Corte del suministro eléctrico	Equipos de climatización	0	8	0	0	6,4	0	1,9
R92	Repudio	Computadores personales	0	0	10	0	0	5	1,5
R113	Errores de los usuarios	Computadores personales	2,5	0,8	1	2	0,6	0,8	1,2
R99	Condiciones inadecuadas de temperatura o humedad	Computadores personales	0	8	0	0	4	0	1,2
R100	Robo de equipos	Computadores personales	0	8	0	0	4	0	1,2
RIESGOS DE PRIORIDAD MUY BAJA									
R105	Manipulación del hardware	Computadores personales	5	6	0	2,5	3	0	1,9
R88	Corte del suministro eléctrico	Fotocopiadoras multifuncionales	0	7	0	0	5,6	0	1,7

R89	Denegación de servicio	Fotocopiadoras multifuncionales	0	7	0	0	5,6	0	1,7
R96	Revelación de la información	Computadores personales	5	0	0	4	0	0	1,6
R15	Enfermedad	Personal	0	9	0	0	4,5	0	1,4
R114	Manipulación del hardware	Fotocopiadoras multifuncionales	4	3,5	0	2	1,8	0	1,3
R102	Revelación de la información	Fotocopiadoras multifuncionales	4	0	0	3,2	0	0	1,3
R97	Manipulación de los registros de actividad (log)	Computadores personales	0	0	5	0	0	4	1,2
R98	Modificación de la información	Computadores personales	0	0	5	0	0	4	1,2
R120	Vulnerabilidades de los programas (software)	SIVRI	2	0,1	2	1,6	0,1	1,6	1,1
R121	Vulnerabilidades de los programas (software)	Computadores personales	2	0,1	2	1,6	0,1	1,6	1,1
R23	Avería de origen físico o lógico	SIVRI	0	4,5	0	0	3,6	0	1,1
R101	Condiciones inadecuadas de temperatura o humedad	Fotocopiadoras multifuncionales	0	7	0	0	3,5	0	1,1
R125	Manipulación del hardware	Servidores	5	4,5	0	1,5	1,4	0	1
R131	Errores del administrador del sistema	Redes de área local	2	2	2	1	1	1	1
R130	Errores del administrador del sistema	SIVRI	2	1,8	2	1	0,9	1	1
R132	Errores del administrador del sistema	Servidores	2	1,8	2	1	0,9	1	1
R124	Manipulación de hardware	Dispositivos de almacenamiento digital	5	0	4	1,5	0	1,2	1

Tabla C.5. Resultados de la estimación del riesgo

Cabe mencionar que, por medio de las dependencias, el riesgo se propagó, desde estos activos inferiores, listados por la Tabla C.5, hacia los activos esenciales. Gracias

al apoyo de la herramienta PILAR, fue posible determinar el nivel de riesgo al que se encontraban sometidos los activos esenciales como consecuencia de las amenazas que afectaban a los demás activos, contemplados por la Tabla C.5. Los resultados son presentados, a continuación, por la Tabla C.6.

Escala para el nivel de riesgo				
Crítico	Alto	Medio	Bajo	Despreciable

C=Confidencialidad I=Integridad D=Disponibilidad P=Ponderado

Activo Esencial	Riesgo			
	C	D	I	P
Presupuesto global de cada proyecto de investigación	7,2	3,9	3,6	5,1
Avales concedidos a cada proyecto de investigación.	8	5	3,6	5,8
Actas de reunión del Consejo de Investigaciones y del Comité de Ética.	6,4	3,92	3,6	4,8
Convenios - Contratos con entidades financiadoras	8	5,6	3,6	6
Documentos de viabilidad financiera de los proyectos de investigación.	8	5	3,2	5,7
Oficios remisorios a las entidades externas financiadoras.	7,2	3,3	3,2	4,9
Oficios remisorios a la División de Gestión Financiera.	6,4	1,6	2,5	3,8
Informes financieros sobre la ejecución presupuestal de los proyectos de investigación.	8	5	3,2	5,7
Informes técnicos, parciales o finales, de los proyectos de investigación.	6,4	3,9	3,2	4,7
Actas de Liquidación de convenios-contratos con entidades externas.	1,6	3,9	3,2	2,8
Certificados de Disponibilidad Presupuestal (CDP)	8	5,6	3,2	5,9
Ordenes de Prestación de Servicios (OPS)	8	5	3,2	5,7
Solicitud de avance para compras o comisión de servicios	6,4	5	2,5	4,8
Orden de suministros	8	3,9	2,5	5,1
Registros de Disponibilidad Presupuestal	8	5,6	3,2	5,9
Órdenes de Pago	8	5,6	3,6	6
Servicio de secretaría	0	5	0	1,5
Servicio de apoyo al Investigador	0	5	0	1,5

Tabla C.6. Nivel de riesgo en los activos esenciales

C.4. Resultados de la caracterización de las salvaguardas

C.4.1. Identificación de las salvaguardas necesarias

Como resultado de la selección de las salvaguardas necesarias para mitigar el riesgo al que se exponen los activos vinculados al caso de estudio, se obtuvo el *Plan de Tratamiento de Riesgos (PTR)*, el cual es expuesto, a continuación, por la Tabla C.7.

ID Riesgo	Amenaza	Activo	Opción de tratamiento	Objetivo de control	Controles
RIESGOS DE ALTA PRIORIDAD					
R1	Ingeniería social (picaresca)	Personal	Modificación	A.6.1	A.6.1.4
R2	Acceso no autorizado	Dispositivos almacenamiento digital	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.8.3	A.8.3.1, A.8.3.2, A.8.3
				A.10.1	A.10.1.1, A.10.1.2
				A.11.2	A.11.2.1, A.11.2.4, A.11.2.5, A.11.2.7
				A.12.1	A.12.1.1, A.12.1.2, A.12.1.4
				A.12.7	A.12.7.1
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
				A.18.1	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
R3	Acceso no autorizado	Documentos físicos	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.7.3	A.7.3.1

				A.8.1	A.8.1.2
				A.8.2	A.8.2.2, A.8.2.3
				A.11.1	A.11.1.1, A.11.1.2, 11,1,3, A.11.1.5, A.11.1.6
				A.12.1	A.12.1.1, A.12.1.2
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
				A.18.1	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4
R4	Revelación de la información	SIVRI	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.7.3	A.7.3.1
				A.9.1	A.9.1.1, A.9.1.2
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6
				A.9.3	A.9.3.1
				A.9.4	A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5
				A.12.1	A.12.1.1, A.12.1.2, A.12.1.4
				A.12.2	A.12.2.1
				A.12.5	A.12.5.1
				A.12.6	A.12.6.1, A.12.6.2
				A.12.7	A.12.7.1
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
				A.13.2	A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4
				A.14.1	A.14.1.1, A.14.1.2, A.14.1.3
				A.14.2	A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9
				A.14.3	A.14.3.1
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4,

					A.16.1.5, A.16.1.6, A.16.1.7
				A.18.1	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
R5	Revelación de la información	Documentos físicos	Modificación	A.6.1	A.6.1.1
				A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.1.6
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
				A.18.1	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4
R6	Destrucción información	Documentos físicos	Modificación	A.6.1	A.6.1.3
				A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.8.2	A.8.2.2, A.8.2.3
				A.12.1	A.12.1.1, A.12.1.2
				A.12.3	A.12.3.1
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
				A.18.1	A.18.1.2, A.18.1.3, A.18.1.4
R7	Acceso no autorizado	SIVRI	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.7.3	A.7.3.1
				A.8.1	A.8.1.2
				A.9.1	A.9.1.1, A.9.1.2
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6

				A.9.3	A.9.3.1
				A.9.4	A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5
				A.10.1	A.10.1.1, A.10.1.2
				A.12.1	A.12.1.4
				A.12.2	A.12.2.1
				A.12.6	A.12.6.1
				A.12.7	A.12.7.1
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
				A.13.2	A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4
				A.14.1	A.14.1.1, A.14.1.2, A.14.1.3
				A.14.2	A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9
				A.14.3	A.14.3.1
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
				A.18.1	A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
R8	Manipulación de programas	SIVRI	Modificación	A.7.1	A.7.1.1, A.7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.7.3	A.7.3.1
				A.8.1	A.8.1.2
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6
				A.9.3	A.9.3.1
				A.9.4	A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5
				A.10.1	A.10.1.1
				A.11.2	A.11.2.9
				A.12.2	A.12.2.1
				A.12.7	A.12.7.1
				A.13.1	A.13.1.1, A.13.1.2

				A.14.2	A.14.2.2, A.14.2.3, A.14.2.4
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R9	Extorsión	Personal	Modificación	A.6.1	A.6.1.3
R10	Suplantación de la identidad	SIVRI	Modificación	A.7.1	A.7.1.1, A.7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.7.3	A.7.3.1
				A.8.1	A.8.1.2
				A.9.2	A.9.2.4
				A.9.3	A.9.3.1
				A.9.4	A.9.4.2, A.9.4.3, A.9.4.4
				A.10.1	A.10.1.1, A.10.1.2
				A.12.2	A.12.2.1
				A.12.5	A.12.5.1
				A.12.6	A.12.6.1
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
				A.13.2	A.13.2.1, A.13.2.2, A.13.2.3
				A.14.1	A.14.1.1, A.14.1.2, A.14.1.3
				A.14.2	A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
				A.18.1	A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
R11	Robo de documentos	Documentos físicos	Modificación	A.6.1	A.8.1.2
				A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.1.6
				A.11.2	A.11.2.5

				A.12.3	A.12.3.1
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R12	Robo de equipos	Dispositivos de almacenamiento digital	Modificación	A.6.1	A.6.1.1, A.6.1.3
				A.6.2	A.6.2.1
				A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.1.6
				A.11.2	A.11.2.1, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.9
				A.12.3	A.12.3.1
				A.12.4	A.12.4.1
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R14	Repudio (negación de actuaciones)	SIVRI	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.7.3	A.7.3.1
				A.9.2	A.9.2.3, A.9.2.6
				A.9.4	A.9.4.2, A.9.4.4, A.9.4.5
				A.10.1	A.10.1.1, A.10.1.2
				A.12.4	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4
				A.12.6	A.12.6.1, A.12.6.2
				A.14.1	A.14.1.2, A.14.1.3
				A.14.2	A.14.2.1, A.14.2.3, A.14.2.5, A.14.2.8, A.14.2.9
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R13	Suplantación de la identidad	Documentos físicos	Reducción	A.6.1	A.6.1.3
				A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.1

				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.1.6
				A.12.3	A.12.3.1
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R16	Destrucción Intencional de la información	SIVRI	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.3
				A.9.1	A.9.1.2
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6
				A.9.3	A.9.3.1
				A.9.4	A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5
				A.12.1	A.12.1.4
				A.12.3	A.12.3.1
				A.12.6	A.12.6.1, A.12.6.2
				A.12.7	A.12.7.1
				A.14.2	A.14.2.1, A.14.2.5, A.14.2.8
				A.17.2	A.17.2.1
R18	Errores de los usuarios	Dispositivos de almacenamiento digital	Modificación	A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.2	A.8.2.3
				A.8.3	A.8.3.1
				A.12.1	A.12.1.1, A.12.1.2
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.5, A.16.1.5, A.16.1.6
R19	Modificación Intencionada de la información	SIVRI	Modificación	A.7.1	A.7.1.1, A.7.1.2
				A.7.2	A.7.2.1, A.7.2.3
				A.9.1	A.9.1.2
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6
				A.9.3	A.9.3.1
				A.9.4	A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5

				A.12.1	A.12.1.4
				A.12.6	A.12.6.1, A.12.6.2
				A.14.1	A.14.1.2, A.14.1.3
				A.14.2	A.14.2.1, A.14.2.5, A.14.2.8
				A.12.3	A.12.3.1
				A.12.7	A.12.7.1
R20	Repudio	Dispositivos de almacenamiento digital	Modificación	A.10.1	A.10.1.1
				A.12.4	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4
				A.12.7	A.12.7.1
R21	Modificación de la información	Dispositivos de almacenamiento digital	Modificación de riesgo	A.8.3	A.8.3, A.8.3.1
				A.9.1	A.9.1.1,
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4
				A.9.3	A.9.3.1
				A.9.4	A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5
				A.10.1	A.10.1.1, A.10.1.2
				A.12.2	A.12.2.1
				A.12.7	A.12.7.1
R24	Pérdida de equipos	Dispositivos de almacenamiento digital	Modificación	A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.1, A.8.1.2, A.8.1.4
				A.11.2	A.11.2.5, A.11.2.6
RIESGOS DE PRIORIDAD MEDIA					
R33	Denegación de servicio	Redes de área local	Transferencia	El riesgo se debería transferir a otra parte que cuente con la capacidad de gestionar de manera más eficaz el riesgo en cuestión.	
R34	Acceso no autorizado	Servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.3
				A.7.3	A.7.3.1
				A.9.1	A.9.1.2
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6
				A.9.3	A.9.3.1

				A.9.4	A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5
				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.6
				A.11.2	A.11.2.1, A.11.2.9
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
R36	Modificación Intencionada de la información	Satélite	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.3
				A.8.2	A.8.2.3
				A.9.2	A.9.2.5, A.9.2.6
				A.11.2	A.11.2.1, A.11.2.5
R37	Corte del suministro eléctrico	Redes de área local	Transferencia	El riesgo se debería transferir a otra parte que cuente con la capacidad de gestionar de manera más eficaz el riesgo en cuestión.	
R38	Acceso no autorizado	Redes de área local	Transferencia		
R39	Corte del suministro eléctrico	Servidores	Modificación	A.11.1	A.11.1.4
				A.11.2	A.11.2.1, A.11.2.2
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R40	Denegación de servicio	Servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.11.2	A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.11.2.9
				A.12.1	A.12.1.3, A.12.1.4
				A.12.2	A.12.2.1
				A.12.4	A.12.4.1, A.12.4.3
				A.12.6	A.12.6.1
				A.12.7	A.12.7.1
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
				A.17.2	A.17.2.1
R41		Satélite	Modificación	A.7.1	A.7.1.1, A7.1.2

	Destrucción Intencionada de la información			A.7.2.	A.7.2.1, A.7.2.3
				A.8.2	A.8.2.3
				A.9.2	A.9.2.5, A.9.2.6
				A.11.2	A.11.2.1, A.11.2.5
				A.12.3	A.12.3.1
				A.17.2	A.17.2.1
R42	Uso no previsto	Redes de área local	Transferencia	El riesgo se debería transferir a otra parte que cuente con la capacidad de gestionar de manera más eficaz el riesgo en cuestión.	
R43	Manipulación de programas	Servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.9.2	A.9.2.6
				A.9.3	A.9.3.1
				A.9.4	A.9.4.5
				A.10.1	A.10.1.1
				A.11.2	A.11.2.9
				A.12.1	A.12.1.4
				A.12.7	A.12.7.1
				A.14.2	A.14.2.2, A.14.2.4, A.14.2.6
R44	Abuso de privilegios de acceso	Servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2, A.8.1.3
				A.12.1	A.12.1.4
				A.12.4	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4
				A.12.7	A.12.7.1
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R45	Uso no previsto	Cuarto de servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2, A.8.1.3
				A.12.1	A.12.1.1, A.12.1.4
R46			Modificación	A.7.1	A.7.1.1, A7.1.2

	Uso no previsto	Almacenes Satélite		A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2, A.8.1.3
				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3
				A.12.1	A.12.1.1
R47	Acceso no autorizado	Almacenes Satélite	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.3
				A.7.3	A.7.3.1
				A.9.1	A.9.1.1
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6
				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.5, A.16.1.5, A.16.1.6
R48	Acceso no autorizado	Cuarto de servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.6
				A.12.1	A.12.1.4
				A.12.7	A.12.7.1
R49	Uso no previsto	Servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2, A.8.1.3
				A.12.1	A.12.1.1, A.12.1.4
R50	Repudio (negación de actuaciones)	Servidores	Modificación	A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.10.1	A.10.1.1
				A.12.4	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4
				A.12.7	A.12.7.1
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R51	Manipulación de hardware	Redes de área local	Transferencia	El riesgo se debería transferir a otra parte que cuente con la capacidad de gestionar de	

				manera más eficaz el riesgo en cuestión.	
R52	Condiciones inadecuadas de temperatura o humedad	Servidores	Modificación	A.6.1	A.6.1.1
				A.11.1	A.11.1.4
				A.11.2	A.11.2.1
R53	Suplantación de la identidad	Servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.9.2	A.9.2.4
				A.9.3	A.9.3.1
				A.9.4	A.9.4.2, A.9.4.3, A.9.4.4
				A.10.1	A.10.1.1, A.10.1.2
				A.11.2	A.11.2.1, A.11.2.9
				A.12.2	A.12.2.1
				A.12.6	A.12.6.1
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R58	Revelación de la información	Servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.7.3	A.7.3.1
				A.9.1	A.9.1.1, A.9.1.2
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6
				A.9.4	A.9.4.1, A.9.4.2, A.9.4.4, A.9.4.5
				A.10.1	A.10.1.1, A.10.1.2
				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3, A.1.1.5
				A.11.2	A.11.2.1, A.11.2.9
				A.12.1	A.12.1.4
				A.12.6	A.12.6.1, A.12.6.2
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
R59		Servidores	Modificación	A.7.1	A.7.1.1, A7.1.2

	Manipulación de los registros de actividad (log)			A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.11.2	A.11.2.1, A11.2.9
				A.12.1	A.12.1.4
				A.12.2	A.12.2.1
				A.12.4	A.12.4.2, A.12.4.3
				A.12.6	A.12.6.1
				A.12.7	A.12.7.1
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R60	Difusión de software dañino	Servidores	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.12.2	A.12.2.1
				A.12.6	A.12.6.1, A.12.6.2
R64	Daños por agua	Almacenes Satélite	Evitación	El estándar ISO/IEC 27005 sugiere que evitar los riesgos causados por la naturaleza puede ser una alternativa más eficaz. Se debería evaluar la posibilidad de transferir físicamente los almacenes a un lugar controlado donde no exista el riesgo	
R72	Manipulación de los ficheros de configuración	Servidores	Modificación	A.7.1	A.7.1.1, A.7.1.2,
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.9.2	A.9.2.4, A.9.2.6
				A.9.3	A.9.3.1
				A.9.4	A.9.4.2, A.9.4.3, A.9.4.4
				A.11.2	A.11.2.1, A.11.2.4, A.11.2.9
				A.12.1	A.12.1.2, A.12.1.4
				A.12.4	A.12.4.1, A.12.4.3
				A.12.6	A.12.6.1, A.12.6.2
				A.12.7	A.12.7.1
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3

				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.5, A.16.1.5, A.16.1.6
RIESGOS DE PRIORIDAD BAJA					
R78	Acceso no autorizado	Computadores personales	Modificación	A.6.1	A.6.1.3
				A.7.1	A.7.1.1, A.7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.7.3	A.7.3.1
				A.8.1	A.8.1.3, A.8.1.4
				A.8.2	A.8.2.3
				A.9.1	A.9.1.1, A.9.1.2
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6
				A.9.4	A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5
				A.11.2	A.11.2.1, A.11.2.4
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.5, A.16.1.5, A.16.1.6
R79	Difusión de software dañino	Computadores personales	Modificación	A.6.1	A.6.1.3
				A.7.1	A.7.1.1, A.7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.9.1	A.9.1.1, A.9.1.2
				A.9.2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6
				A.9.3	A.9.3.1
				A.9.4	A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5
				A.11.2	A.11.2.1, A.11.2.4
				A.12.2	A.12.2.1
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.5, A.16.1.5, A.16.1.6
R80	Manipulación de programas	Computadores personales	Modificación	A.7.1	A.7.1.1, A.7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.9.2	A.9.2.6
				A.9.3	A.9.3.1

				A.9.4	A.9.4.4, A.9.4.5
				A.10.1	A.10.1.1
				A.11.2	A.11.2.8, A.11.2.9
				A.12.1	A.12.1.4
				A.12.7	A.12.7.1
				A.14.2	A.14.2.2, A.14.2.4, A.14.2.6
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6
R81	Abuso de privilegios de acceso	Computadores personales	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2, A.8.1.3
				A.11.2	A.11.2.5
				A.12.1	A.12.1.4
				A.12.4	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4
				A.12.7	A.12.7.1
				A.16.1	A.16.1.2, A.16.1.3,A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R82	Uso no previsto	Computadores personales	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2, A.8.1.3
				A.11.2	A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9
				A.12.1	A.12.1.1, A.12.1.4
				A.12.6	A.12.6.2
				A.12.7	A.12.7.1
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R83	Acceso no autorizado	Fotocopiadora multifuncional	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.8.2	A.8.2.3
				A.9.1	A.9.1.2
				A.11.2	A.11.2.1, A.11.2.8
				A.12.1	A.12.1.4
				A.12.7	A.12.7.1

				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R84	Uso no previsto	Fotocopiadora multifuncional	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2, A.8.1.3
				A.12.1	A.12.1.1, A.12.1.4
				A.12.7	A.12.7.1
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R85	Corte del suministro eléctrico	Computadores personales	Modificación	A.6.1	A.6.1.4
				A.11.1	A.11.1.4
				A.11.2	A.11.2.1, A.11.2.2
				A.16.1	A.16.1.2, A.16.1.3,A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R86	Denegación de servicio	Computadores personales	Modificación	A.8.1	A.8.1.2
				A.12.2	A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.11.2.5, A.11.2.8, A.11.2.9
				A.12.1	A.12.1.3, A.12.1.4
				A.12.2	A.12.2.1
				A.12.6	A.12.6.1, A.12.6.2
				A.12.7	A.12.7.1
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R87	Corte del suministro eléctrico	Equipos de climatización	Modificación	A.6.1	A.6.1.4
				A.11.1	A.11.1.4
				A.11.2	A.11.2.1, A.11.2.2
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R90	Uso no previsto	Oficinas del personal	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3

				A.8.1	A.8.1.2, A.8.1.3
				A.12.1	A.12.1.1
R91	Acceso no autorizado	Oficinas del personal	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.11.1	A.11.1.2, A.11.1.3, A.11.1.6
				A.12.1	A.12.1.1, A.12.1.4
				A.12.7	A.12.7.1
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R92	Repudio (negación de actuaciones)	Computadores personales	Modificación	A.10.1	A.10.1.1
				A.12.4	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4
				A.12.7	A.12.7.1
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R93	Suplantación de la identidad	Computadores personales	Modificación	A.7.1	A.7.1.1, A7.1.2
				A.7.2.	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.2
				A.9.2	A.9.2.4
				A.9.3	A.9.3.1
				A.9.4	A.9.4.2, A.9.4.3, A.9.4.4
				A.10.1	A.10.1.1, A.10.1.2
				A.11.2	A.11.2.1, A.11.2.6, A.11.2.8, A.11.2.9
				A.12.2	A.12.2.1
				A.12.6	A.12.6.1
				A.13.1	A.13.1.1, A.13.1.2, A.13.1.3
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R99	Condiciones inadecuadas de	Computadores personales	Modificación	A.6.1	A.6.1.1
				A.11.1	A.11.1.4
				A.11.2	A.11.2.1

	temperatura o humedad				
R100	Robo de equipos	Computadores personales	Modificación	A.6.1	A.6.1.3
				A.7.1	A.7.1.1, A7.1.2
				A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.1	A.8.1.1, A.8.1.2, A.8.1.4
				A.11.1	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.1.6
				A.11.2	A.11.2.1, A.11.2.5, A.11.2.6
				A.16.1	A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
R106	Daños por agua	Oficinas del personal	Evitación	El estándar ISO/IEC 27005 sugiere que evitar los riesgos causados por la naturaleza puede ser una alternativa más eficaz. Se debería evaluar la posibilidad de transferir físicamente los almacenes a un lugar controlado donde no exista el riesgo	
R113	Errores de los usuarios	Computadores personales	Modificación	A.7.2	A.7.2.1, A.7.2.2, A.7.2.3
				A.8.2	A.8.2.3
				A.11.2	A.11.2.4, A.11.2.6
				A.12.1	A.12.1.1, A.12.1.2
				A.16.1	A.16.1.1, A.16.1.2, A.16.1.3,A.16.1.5, A.16.1.5, A.16.1.6
RIESGOS DE PRIORIDAD MUY BAJA					
R120	Vulnerabilidades de los programas (software)	SIVRI	Retención	Como el riesgo pertenece a la Zona 3, entonces se satisface los criterios para su retención o aceptación. No se debe aplicar ninguna acción ni implementar control alguno.	
R121	Vulnerabilidades de los programas (software)	Computadores personales	Retención		

R124	Manipulación de hardware	Dispositivos de almacenamiento digital	Retención	
R125	Manipulación del hardware	Servidores	Retención	
R130	Errores del administrador del sistema	SIVRI	Retención	
R131	Errores del administrador del sistema	Redes de área local	Retención	
R132	Errores del administrador del sistema	Servidores	Retención	
R15	Enfermedad	Personal	Retención	
R23	Avería de origen físico o lógico	SIVRI	Retención	Como el riesgo pertenece a la Zona 3, entonces se satisface los criterios para su retención o aceptación. No se debe aplicar ninguna acción ni implementar control alguno.
R105	Manipulación del hardware	Computadores personales	Retención	
R88	Corte del suministro eléctrico	Fotocopiadora multifuncional	Retención	
R89	Denegación de servicio	Fotocopiadora multifuncional	Retención	
R96	Revelación de la información	Computadores personales	Retención	
R114	Manipulación del hardware	Fotocopiadora multifuncional	Retención	
R102	Revelación de la información	Fotocopiadora multifuncional	Retención	
R97	Manipulación de los registros de actividad (log)	Computadores personales	Retención	
R98	Modificación de la información	Computadores personales	Retención	
R101	Temperatura inadecuada	Fotocopiadora multifuncional	Retención	

Tabla C.7. PTR

De esta manera se logró satisfacer los entregables: *Plan del tratamiento del Riesgo* y *Lista de controles y objetivos de control seleccionados*, requeridos por la tarea MAR 4.1 y por la cuarta fase del proceso de planeación de un SGSI.

C.4.2. Resultados de la aceptación de riesgos

Como todos los riesgos fueron reducidos al nivel *Despreciable,* de acuerdo con la escala propuesta por la Tabla 5.30, se logró que la dirección aceptara todos los riesgos residuales. Esta decisión es comunicada, de manera escrita, por el jefe de la División de Gestión de Investigación, como lo ilustra a continuación la Figura C.1, logrando satisfacer los entregables: *Aceptación de riesgos residuales* y *Aprobación del Plan de Tratamiento de Riesgos,* requerido por la tarea MARA 4.2 y por la fase 4 del proceso de planeación de un SGSI.

Popayán Cauca, 25 de Mayo de 2015

Señores:
JHON HOLMAN REYES CERÓN
MIGUEL ANGEL GALÍNDEZ MUÑOZ
Estudiantes del programa de Ingeniería de Sistemas
Universidad del Cauca

Asunto: aceptación de los riesgos residuales y aprobación del PTR

Cordial saludo:

En relación con su trabajo de pregrado: *"Gestión del riesgo de SI con base en la norma ISO/IEC 27005:2011 adaptando la metodología MAGERIT V3 para el procedimiento de formulación y ejecución de proyectos con financiación externa"* dirigido por el especialista en redes y servicios telemáticos Siler Amador Donado, me permito comunicarles la aceptación formal de los riesgos residuales y la aprobación del Plan de Tratamiento de Riesgos (PTR).

HELDER MAURICIO CHACÓN VILLOTA
C.C: 10.538.987
Jefe de la División de Gestión de Investigación
Vicerrectoría de Investigaciones
Universidad del Cauca

Figura C.1. Aceptación de riesgos y aprobación del PTR

C.4.3. Declaración de aplicabilidad (SOA)

Como se aceptaron todos los riesgos, se puede concluir que el tratamiento de riesgos fue satisfactorio. A continuación, la Tabla C.8 expone la Declaración de Aplicabilidad (SOA) resultante, en la cual se identifica cuáles de los 144 controles sugeridos por el Anexo A de la norma ISO/IEC 27001 [2] deberán ser implementados en el caso de estudio para mitigar, adecuadamente, los riesgos de la SI previamente identificados, justificando claramente, cualquier inclusión y exclusión de los controles propuestos por el Anexo A.

CONTROL		APLICA	JUSTIFICACIÓN
5.1.1	Conjunto de políticas para la seguridad de la información.	SI	La dirección de la Universidad del Cauca debería brindar orientación y soporte mediante la definición y publicación de las políticas para la SI en el caso de estudio. Dichas políticas deben ser comunicadas a los empleados, a las entidades externas que financian los proyectos de investigación y a las demás terceros.
5.1.2	Revisión de las políticas para la seguridad de la información.	SI	Las políticas que se definan para la SI. en el caso de estudio, deberían ser revisadas a intervalos planeados o si ocurren cambios significativos con el fin de garantizar su conveniencia, adecuación y eficacia continuas
6.1.1	Asignación de responsabilidades para la SI	SI	Se debería definir y asignar todas las responsabilidades de la SI en el caso de estudio
6.1.2	Segregación de tareas	SI	Se deberían separar los deberes y tareas en conflicto con el fin de reducir la probabilidad de uso indebido o modificación no autorizada o no intencional
6.1.3	Contacto con las autoridades.	SI	Se debería mantener el contacto con las autoridades pertinentes para reportar oportunamente cualquier incidente de SI
6.1.4	Contacto con grupos de interés especial.	SI	Se debería mantener contacto con grupos y foros especializados en materia de la SI con el fin de ganar acceso a la asesoría de especialistas, mejorar el conocimiento y recibir alertas e intercambiar información acerca de nuevas tecnologías, amenazas y vulnerabilidades.

6.1.5	Seguridad de la información en la gestión de proyectos	SI	La SI debería ser integrada con los métodos para la gestión de proyectos para garantizar que los riesgos de la SI son identificados y abordados como parte del proyecto.
6.2.1	Política de uso de dispositivos para movilidad.	NO	Para el caso de estudio no se contempla ninguna forma de trabajo a distancia, es decir, todas las actividades se ejecutan al interior de las instalaciones de la VRI. Por ende, resulta completamente innecesario implementar políticas o medidas relacionadas con el teletrabajo.
6.2.2	Teletrabajo.	NO	Para el caso de estudio no se contempla ninguna forma de trabajo a distancia, es decir, todas las actividades se ejecutan al interior de las instalaciones de la VRI. Por ende, resulta completamente innecesario implementar políticas o medidas relacionadas con el teletrabajo.
7.1.1	Investigación de antecedentes.	SI	Se debería emprender una verificación de los antecedentes de los aspirantes a vacantes con el fin de garantizar que éstos son aptos y adecuados para desempeñar los roles en cuestión.
7.1.2	Términos y condiciones de contratación.	SI	Se deberían establecer, mediante acuerdos contractuales, las obligaciones y responsabilidades de los empleados y contratistas frente a la SI en el caso de estudio.
7.2.1	Responsabilidades de gestión.	SI	La Dirección debería exigir a todos los empleados y contratistas, vinculados al caso de estudio, aplicar la SI de acuerdo con las políticas y procedimientos establecidos para tal fin.
7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	El análisis de requerimientos de la SI reveló que el personal, vinculado al caso de estudio, no se encuentra debidamente capacitado en materia de la SI, careciendo del nivel de conocimiento básico en esta área. Dicho análisis concluye que resulta necesario definir e implementar un programa de educación y entrenamiento para garantizar que el personal se encuentre totalmente capacitado y sea consciente de sus responsabilidades frente a la SI.

7.2.3	Proceso disciplinario.	SI	Debería existir un proceso disciplinario formal para emprender acciones contra los empleados y contratistas que cometan violaciones a la SI. El proceso disciplinario deberá ser comunicado a todos los empleados como un elemento disuasorio que prevenga posibles violaciones.
7.3.1	Cese o cambio de puesto de trabajo.	SI	Se deberían definir, comunicar y hacer cumplir los deberes y responsabilidades, de cada empleado, que permanecerán vigentes después de la terminación o cambio del empleo.
8.1.1	Inventario de activos.	SI	Se debería elaborar y mantener un inventario de todos los activos asociados con la información gestionada durante la ejecución del caso de estudio
8.1.2	Propiedad de los activos.	SI	Todo activo debería tener un propietario asignado quien el responsable de velar por su protección durante todo su ciclo de vida.
8.1.3	Uso aceptable de los activos.	SI	Se debería identificar, documentar e implementar un reglamento sobre el uso aceptable de los activos de información, el cual será comunicado a todos los empleados y partes externas vinculadas al caso de estudio.
8.1.4	Devolución de activos.	SI	El proceso de terminación de contratos debería incluir y formalizar la devolución de todos los activos asignados a empleados, contratistas y partes externas vinculadas al caso de estudio.
8.2.1	Directrices de clasificación.	SI	Se debería clasificar la información de acuerdo a su valor, criticidad y su sensibilidad a ser divulgada o manipulada de manera no autorizada. Dicha clasificación debería considerar los 3 tipos de información pública definidos por el artículo 6 de la ley 1712 de 2014.
8.2.2	Etiquetado y manipulado de la información.	SI	Se debería desarrollar e implementar un conjunto de procedimientos para el etiquetado de la información de acuerdo con las directrices de clasificación definidas.
8.2.3	Manipulación de activos.	SI	Se debería desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación adoptado para el caso de estudio.

8.3.1	Gestión de soportes extraíbles.	SI	Procedimientos, para la gestión de dispositivos extraíbles, deberían ser definidos de acuerdo con el esquema de clasificación adoptado para el caso de estudio.
8.3.2	Eliminación de soportes.	SI	Se deben establecer procedimientos formales para la eliminación segura de los dispositivos de almacenamiento con el fin de minimizar el riesgo de que haya fugas de información confidencial.
8.3.3	Soportes físicos en tránsito.	SI	Se deben proteger los medios que contienen información, contra acceso no autorizado, uso indebido o corrupción durante el transporte
9.1.1	Política de control de acceso	SI	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información
9.1.2.	Acceso a redes y servicios	SI	solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
9.2.1	Gestión de altas/bajas en el registro de usuarios.	SI	se debe implementar un proceso formal de registro y de cancelación
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	SI	se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	SI	se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
9.2.4	Gestión de información confidencial de autenticación de usuarios.	SI	la asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal
9.2.5	Revisión de los derechos de acceso de los usuarios.	SI	Los propietarios de los activos deberían revisar, frecuentemente, los derechos que tienen los usuarios para acceder a sus activos para garantizar que nadie tenga derechos privilegiados no autorizados.

9.2.6	Retirada o adaptación de los derechos de acceso	SI	Se deberían retirar los derechos de acceso de todos los empleados y partes externas una vez se haya terminado el empleo, contrato o acuerdo. De igual manera se deberían ajustar los derechos de acceso en respuesta a cualquier cambio en el contrato o empleo.
9.3.1	Uso de información confidencial para la autenticación.	SI	Se le debería exigir a todos los empleados y contratistas, vinculados al caso de estudio, cumplir con las prácticas que disponga la Universidad del Cauca en cuanto al uso de la información secreta de autenticación.
9.4.1	Restricción del acceso a la información.	SI	Se debe restringir el acceso a la información gestionada por el caso de estudio y al sistema de información SIVRI de acuerdo con la política de control de acceso.
9.4.2	Procedimientos seguros de inicio de sesión.	SI	El acceso a las aplicaciones debe ser controlado por un procedimiento seguro de conexión.
9.4.3	Sistema de gestión de contraseñas.	SI	Se debería implementar un sistema de gestión de contraseñas que sea interactivo y garantice la calidad de las contraseñas.
9.4.4	Uso de herramientas de administración de sistemas.	SI	Se debería restringir el uso de software capaz de anular el sistema y los controles de aplicación.
9.4.5	Control de acceso al código fuente de los programas.	SI	Debe restringirse el acceso al código fuente del SIVRI y demás sistemas y aplicaciones.
10.1.1	Política de uso de los controles criptográficos.	SI	Se debe desarrollar e implementar una política sobre el uso de controles de seguridad para proteger la información gestionada por el caso de estudio.
10.1.2	Gestión de claves.	SI	Se debería desarrollar e implementar una política sobre el uso, protección y ciclo de vida de las claves criptográficas, incluyendo la generación, almacenamiento, recuperación, distribución, retirada y destrucción de las mismas.
11.1.1	Perímetro de seguridad física.		Se debería definir y usar perímetros de seguridad para proteger las áreas que contienen o procesan, ya sea, información crítica o sensible
11.1.2	Controles físicos de entrada.	SI	Se debe proteger las entradas de las instalaciones físicas mediante controles

			adecuados para garantizar que solo se permita el acceso a personal autorizado
11.1.3	Seguridad de oficinas, despachos y recursos.	SI	Se debería diseñar y aplicar controles y procedimientos para gestionar la seguridad física de las oficinas, recintos e instalaciones vinculadas al caso de estudio.
11.1.4	Protección contra las amenazas externas y ambientales.	SI	Se debería diseñar y aplicar controles y procedimientos para brindar protección contra desastres naturales, ataques o accidentes. Se debería acudir a especialistas para recibir asesoría sobre cómo evitar los daños causados por fuego, inundaciones, terremotos, explosiones, disturbios y cualquier forma de desastre natural o causado por el hombre.
11.1.5	El trabajo en áreas seguras.	SI	Se debería diseñar y aplicar procedimientos que garantice el trabajo en áreas seguras
11.1.6	Áreas de acceso público, carga y descarga.	SI	Se debería controlar los parqueaderos, recepciones y demás puntos de acceso a los cuales personas no autorizadas puedan ingresar y, en lo posible, aislar dichas zonas de las instalaciones de procesamiento de la información para evitar cualquier forma de acceso no autorizado.
11.2.1	Emplazamiento y protección de equipos.	SI	Debería protegerse y almacenarse los equipos para reducir los riesgos de las amenazas ambientales, así mismo los riesgos de acceso no autorizado.
11.2.2	Instalaciones de suministro.	SI	Los equipos, vinculados al caso de estudio, deberían estar protegidos contra fallos en el suministro de energía y demás interrupciones causadas por fallas en los suministros como las telecomunicaciones, electricidad, agua, gas, aire acondicionado, etc.
11.2.3	Seguridad del cableado.	SI	Debería ser protegido el cableado que soporta los servicios de energía y telecomunicaciones, contra interceptación, interferencia o daños.
11.2.4	Mantenimiento de los equipos.	SI	Los equipos deberían ser mantenidos correctamente para garantizar su continua disponibilidad e integridad. El mantenimiento debe llevarse a cabo de acuerdo a las recomendaciones y especificaciones emanadas por el fabricante de los mismos.

11.2.5	Salida de activos fuera de las dependencias de la empresa.	SI	No debería permitirse la salida de cualquier tipo de activo sin autorización previa.
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	NO	Para el caso de estudio no se contempla ninguna forma de trabajo a distancia. Por ende, resulta completamente innecesario implementar este tipo de controles cuyo propósito sería proteger los activos involucrados en labores fuera de las instalaciones de la VRI.
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	SI	Todos los dispositivos de almacenamiento de información deben ser verificados antes de ser eliminados o reutilizados con el fin de proteger información sensible o licencias de software
11.2.8	Equipo informático de usuario desatendido.	SI	Los usuarios, empleados y contratistas deberían garantizar que los equipos desatendidos reciben la protección apropiada.
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	SI	Debería adoptarse políticas de; escritorio limpio para los papeles y medios extraíbles de almacenamiento, y de pantalla transparente para las instalaciones de procesamiento de información.
12.1.1	Documentación de procedimientos de operación.	SI	Los procedimientos operativos deberían ser documentados y estar disponibles para quien los necesite. Estos deben especificar las instrucciones operacionales sobre las actividades asociadas con el procesamiento de información e instalaciones de comunicaciones.
12.1.2	Gestión de cambios.	SI	Se deberían controlar los cambios en el caso de estudio, sus instalaciones de procesamiento, su sistema de información SIVRI, su sistema de archivo SATÉLITE y demás activos relevantes con el fin de evitar efectos negativos en la SI.
12.1.3	Gestión de capacidades.	SI	Debería ser monitoreado el uso de los recurso, como también, identificar las necesidades de los sistemas y realizar los ajustes necesarios para asegurar el rendimiento de los sistemas que se utilizan para el caso de estudio.

12.1.4	Separación de entornos de desarrollo, prueba y producción.	SI	Los entornos de desarrollo, prueba y producción deberían estar separados para reducir los riesgos de acceso no autorizado y evitar problemas operacionales.
12.2.1	Controles contra el código malicioso.	SI	Se deberían implementar controles para la detección, prevención y recuperación contra malware. Estos controles deben estar acompañados de un nivel apropiado de conciencia y entrenamiento por parte del personal vinculado al caso de estudio
12.3.1	Copias de seguridad de la información.	SI	Se deben realizar copias de seguridad de la información e imágenes de los sistemas de información, además deben realizarse teste de seguridad regularmente a las copias.
12.4.1	Registro y gestión de eventos de actividad.	SI	Los registros de las actividades de los usuarios, excepciones, fallos e información sobre eventos de seguridad, en el caso de estudio, deberían ser producidos, mantenidos y revisados regularmente.
12.4.2	Protección de los registros de información.	SI	Se debería proteger los registros de actividad, y equipos asociados, contra manipulación y acceso no autorizado, pues, si llegaran a ser comprometidos, pueden generarse una falsa sensación de seguridad en el caso de estudio.
12.4.3	Registros de actividad del administrador y operador del sistema.	SI	Los usuarios privilegiados, como los administradores, pueden manipular los registros de actividad para encubrir sus intereses propios. Por ende, resulta necesario que también se registren las actividades de los administradores y operadores de los sistemas. Dichos registros deberán ser protegidos y revisados frecuentemente.
12.4.4	Sincronización de relojes.	SI	La configuración correcta del reloj de los sistemas es importante para garantizar la precisión de los registros de actividad, los cuales pueden ser requeridos, como evidencia, en investigaciones legales o disciplinarias. Por ende, resulta necesario
12.5.1	Instalación del software en sistemas en producción.	SI	Se deberían implementar procedimientos para controlar la instalación de software en los sistemas operacionales.

12.6.1	Gestión de las vulnerabilidades técnicas.	SI	Se debería obtener, de manera oportuna, información acerca de las vulnerabilidades técnicas de SIVRI y los demás sistemas y aplicaciones usados durante la ejecución del caso de estudio. De igual manera se debe evaluar la exposición a dichas vulnerabilidades y adoptar las medidas apropiadas para abordar los riesgos asociados.
12.6.2	Restricciones en la instalación de software.	SI	Se deberían establecer e implementar normas que rijan los mecanismos a seguir para la instalación segura de software
12.7.1	Controles de auditoría de los sistemas de información.	SI	Se debería planificar y acordar requisitos de auditoría y las actividades concernientes a la verificación de los sistemas de información con el fin de minimizar las interrupciones al procedimiento.
13.1.1	Controles de red.	SI	Las redes de comunicaciones deberían ser gestionadas y controladas con el fin de proteger la información tratada por el SIVRI y demás sistemas y aplicaciones usados durante la ejecución del caso de estudio.
13.1.2	Mecanismos de seguridad asociados a servicios en red.	SI	Se deberían identificar los mecanismos de seguridad, niveles de servicio y requerimientos de la Dirección para todos los servicios de red. Esto deberá ser incluido en los acuerdos pactados con los proveedores de servicios y debe ser objeto de monitoreo continuo para garantizar su debido cumplimiento.
13.1.3	Segregación de redes.	SI	Un método para gestionar la seguridad de las redes es dividirlas en dominios de red separados con base en el nivel de confianza: dominio público, dominio de servidores, etc. Por ende, resulta necesario segregar servicios, usuarios y sistemas de información en diferentes dominios de red.
13.2.1	Políticas y procedimientos de intercambio de información.	SI	Se debería desarrollar e implementar políticas formales para proteger la información objeto de transmisión o intercambio.
13.2.2	Acuerdos de intercambio.	SI	Los acuerdos deberían abordar la transferencia segura de información entre la organización y las partes externas referenciando los controles las políticas,

			procedimientos y estándares necesarios para proteger la información que será intercambiada.
13.2.3	Mensajería electrónica.	SI	Debe estar adecuadamente protegida la información involucrada en mensajería electrónica
13.2.4	Acuerdos de confidencialidad y secreto.	SI	Se debería identificar, documentar y revisar regularmente requisitos que cubran las necesidades en el caso de estudio para la protección de la información.
14.1.1	Análisis y especificación de los requisitos de seguridad.	SI	Los requerimientos relacionados con la SI deberían ser incluidos en los requerimientos de proyectos para la mejora de SIVRI y/o el desarrollo de nuevos sistemas de información.
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	SI	Se debe proteger la información que requiera servicios de aplicaciones que son accedidos mediante redes públicas, contra toda actividad fraudulenta, divulgación no autorizada y/o modificación.
14.1.3	Protección de las transacciones por redes telemáticas.	SI	La información involucrada en transacciones, realizadas por las diferentes aplicaciones, debería ser protegida con el fin de prevenir transmisiones incompletas, enrutamiento errado, manipulación, divulgación, duplicado y retransmisión no autorizadas de mensajes
14.2.1	Política de desarrollo seguro de software.	SI	Se debería diseñar e implementar regla que aseguren el desarrollo de software seguro al interior de la VRI
14.2.2	Procedimientos de control de cambios en los sistemas.	SI	Los cambios a SIVRI y demás sistemas dentro, del ciclo de vida del desarrollo, debería ser controlado mediante el uso de procedimientos formales para el control de cambios.
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	SI	Se deben realizar revisiones y pruebas a las operaciones críticas del caso de estudio tras ejecutar cambios en plataformas relacionadas a este
14.2.4	Restricciones a los cambios en los paquetes de software.	SI	Toda modificación a los paquetes de software debería ser rechazada. Si la necesidad lo amerita, los cambios deberán ser estrictamente controlados.
14.2.5	Uso de principios de ingeniería en	SI	Se debería establecer, documentar, mantener y aplicar los principios de la

	protección de sistemas.		ingeniería de sistemas seguros a cualquier esfuerzo de implementación.
14.2.6	Seguridad en entornos de desarrollo.	SI	Se debería proteger adecuadamente los entornos de desarrollo que cubren la integración y todo el ciclo de vida de los sistemas de Información para el caso de estudio
14.2.7	Externalización del desarrollo de software.	NO	El desarrollo de los sistemas de información y aplicaciones usados por el caso de estudio, es llevado a cabo por el mismo personal de la VRI con el fin de evitar la necesidad de desarrollos externalizados. Razón por la cual, este control se considera completamente innecesario.
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	SI	Deberían llevarse a cabo pruebas de funcionalidad durante el desarrollo al interior de la VRI
14.2.9	Pruebas de aceptación.	SI	Debería establecer un conjunto de pruebas de aceptación y criterios relacionados para nuevos sistemas de información o actualizaciones de sistemas ya existentes como el caso de SIVRI
14.3.1	Protección de los datos utilizados en pruebas.	SI	Los datos de prueba deberían ser cuidadosamente seleccionados, protegidos y controlados.
15.1.1	Política de seguridad de la información para suministradores.	NO	El jefe de la División de Gestión de la Investigación, responsable de la ejecución del caso de estudio, manifiesta que este procedimiento no acude a ningún proveedor. Por esta razón, este control resulta completamente innecesario.
15.1.2	Tratamiento del riesgo dentro de acuerdo	NO	El jefe de la División de Gestión de la Investigación, responsable de la ejecución del caso de estudio, manifiesta que este procedimiento no acude a ningún proveedor. Por esta razón, este control resulta completamente innecesario.
15.1.3.	Cadena de suministro en tecnologías de la información y comunicaciones	NO	El jefe de la División de Gestión de la Investigación, responsable de la ejecución del caso de estudio, manifiesta que este procedimiento no acude a ningún proveedor. Por esta razón, este control resulta completamente innecesario.

15.2.1	Supervisión y revisión de los servicios prestados por terceros.	NO	El jefe de la División de Gestión de la Investigación, responsable de la ejecución del caso de estudio, manifiesta que este procedimiento no acude a ningún proveedor. Por esta razón, este control resulta completamente innecesario.
15.2.2	Gestión de cambios en los servicios prestados por terceros.	NO	El jefe de la División de Gestión de la Investigación, responsable de la ejecución del caso de estudio, manifiesta que este procedimiento no acude a ningún proveedor. Por esta razón, este control resulta completamente innecesario.
16.1.1	Responsabilidades y procedimientos.	SI	Se debería establecer responsabilidades y procedimientos para la gestión, para garantizar una respuesta rápida a los incidentes de seguridad de la información
16.1.2	Notificación de los eventos de seguridad de la información.	SI	Todos los empleados y contratistas deberían ser conscientes de su responsabilidad de reportar, lo más pronto posible, cualquier evento de SI.
16.1.3	Notificación de puntos débiles de la seguridad.	SI	Los empleados de la VRI que manipulan el SIVRI o un futuro nuevo sistema de información deberían estar obligados a reportar cualquier anomalía o deficiencia de seguridad de la información.
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	SI	Se debería valorar cada evento reportado y determinar si se debe clasificar como un incidente de SI con el fin de identificar el impacto y el grado de los mismos.
16.1.5	Respuesta a los incidentes de seguridad.	SI	Se debería dar respuesta a los incidentes de SI de acuerdo a los procedimientos documentados.
16.1.6	Aprendizaje de los incidentes de seguridad de la información.	SI	Los conocimientos adquiridos mediante el análisis solución de incidentes de seguridad de la información deberían utilizarse para reducir las probabilidades e impacto de los mismos en el futuro
16.1.7	Recopilación de evidencias.	SI	Se debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información

			que pueda servir como evidencia para propósitos disciplinarios y acciones legales..
17.1.1	Planificación de la continuidad de la SI.	SI	Se debería determinar los requerimientos para la continuidad de gestión de la SI en situaciones adversas
17.1.2	Implantación de la continuidad de la seguridad de la información.	SI	Se debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar la continuidad de las operaciones del caso de estudio cuando se presenten situaciones adversas.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	Los controles implementados para la continuidad de la SI deberían ser verificados a intervalos regulares con el fin de garantizar que estos son válidos y efectivos durante situaciones adversas
17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	SI	Las instalaciones de procesamiento de información deberían ser implementadas con la suficiente redundancia como para lograr los requerimientos de disponibilidad.
18.1.1	Identificación de la legislación aplicable.	SI	Se deberían identificar, documentar y actualizar todos los acuerdos regulatorios y contractuales que rigen para el caso de estudio
18.1.2	Derechos de propiedad intelectual (DPI).	SI	Se debería implementar los procedimientos apropiados para garantizar el cumplimiento de los requerimientos legales, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de software propietario.
18.1.3	Protección de los registros de la organización.	SI	Se deberían establecer mecanismos de protección de los registros de la VRI contra pérdida, destrucción, falsificación y divulgación no autorizado conforme a los requisitos legales, reglamentarios, contractuales y requerimientos de negocio de la Universidad.
18.1.4	Protección de datos y privacidad de la información personal.	SI	Se debería garantizar la privacidad y protección de la información de identificación personal según lo requieran las leyes aplicables.
18.1.5	Regulación de los controles criptográficos.	SI	Se debería utilizar controles criptográficos para dar cumplimiento a todos los acuerdos pertinentes; leyes y reglamentos.

18.2.1	Revisión independiente de la seguridad de la información.	SI	El enfoque para gestionar la SI y su implementación deberían ser revisados a intervalos planeados o cuando ocurran cambios significativos.
18.2.2	Cumplimiento de las políticas y normas de seguridad.	SI	La dirección debe revisar periódicamente el cumplimiento de la política de seguridad de la información y el conjunto de reglamentos relacionados con la seguridad de la información
18.2.3	Comprobación del cumplimiento.	SI	Se debería revisar regularmente los sistemas de información para garantizar que éstos cumplen con las políticas de SI y demás estándares definidos por la Universidad del Cauca

Tabla C.8. Declaración de Aplicabilidad (SOA)

Anexo D.

Evidencias de la evaluación de la solución

D.1. Evaluación de expertos

A continuación, la Tabla D.1 expone el resultado de la evaluación de la adaptación por parte de la Ingeniera Betty Fernández, funcionaria del Área de Servidores y Servicios de Internet adscrita a la División de Tecnologías de la Información y las Comunicaciones de la Universidad del Cauca.

ELEMENTO DE LA ADAPTACIÓN QUE SE VA A EVALUAR	CALIFICACIÓN
Esquema para la clasificación de la información	① ● ③ ④ ⑤
	Observaciones: Según la ley de Hábeas Data, los datos pueden ser públicos, semiprivados o privados. Su esquema, por lo contrario, define 3 tipos: información pública reservada, información pública clasificada e información pública. Les sugiero que realicen un mapeo que evidencie el cumplimiento de lo establecido por la ley de Hábeas Data.
Organización para la gestión del riesgo	① ② ● ④ ⑤
	Observaciones: A pesar de que articularon los roles y responsabilidades con la estructura de la Universidad, olvidaron considerar el Área de Servidores y Servicios de Internet. Tengan en cuenta que ésta área juega un papel crítico en el desarrollo de casi todas las actividades de la Universidad y, por ende, merecería ser incluida en su organización para la gestión de riesgos.

Criterios para la valoración de los activos	① ② ③ ④ ●
	Observaciones: No tengo observaciones para este aspecto
Criterios para la valoración de las amenazas	① ② ● ④ ⑤
	Observaciones: Para calcular la probabilidad de ocurrencia analizan la probabilidad de que la amenaza se materialice sin intervención y la probabilidad de que un atacante la materialice, pero no consideran que la motivación/interés del atacante en materializar la amenaza también representa un factor influyente.
Criterios para la evaluación del riesgo	① ② ③ ④ ●
	Observaciones: No tengo observaciones al respecto
Criterios para la valoración de las salvaguardas	① ② ③ ● ⑤
	Observaciones: A mi parecer, el nivel de eficacia asignado a la madurez L3 se encuentra muy alto (90%). Creo que debería tener, cuando mucho, un 75% pues el hecho de que un control/procedimiento esté documentado no quiere decir que sea del todo eficaz. Lo será cuando éste, por lo menos, sea sometido a medición mediante indicadores (madurez L4) para su posterior mejora (madurez L5).
Criterios para el tratamiento de riesgos	① ② ③ ④ ●
	Observaciones: No tengo observaciones al respecto
Aceptación de riesgos	① ② ③ ④ ●
	Observaciones: Sin observaciones al respecto

Tabla D.1. Evaluación por parte de un experto

A continuación, la Tabla D.2 expone el resultado de la evaluación de la adaptación por parte del Ingeniero Adolfo Eduardo García Muñoz, funcionario del Área de Sistemas de la Vicerrectoría de Investigaciones de la Universidad del Cauca.

ELEMENTO DE LA ADAPTACIÓN QUE SE VA A EVALUAR	CALIFICACIÓN
Esquema para la clasificación de la información	① ② ③ ④ ⑤ Respuesta: 5
	Observaciones:
Organización para la gestión del riesgo	① ② ③ ④ ⑤ Respuesta: 5
	Observaciones:
Criterios para la valoración de los activos	① ② ③ ④ ⑤ Respuesta: 3
	Observaciones: Los criterios definidos le dan un valor muy bajo a la información pública. Sean más generosos en este aspecto. El hecho de que la información sea pública no quiere decir que ésta sea irrelevante o prescindible.
Criterios para la valoración de las amenazas	① ② ③ ④ ⑤ Respuesta: 4
	Observaciones: Veo que usaron los criterios de otra metodología… ¿verificaron que se podían articular o integrar con su adaptación?
Criterios para la evaluación del riesgo	① ② ③ ④ ⑤ Respuesta: 2
	Observaciones: los criterios definidos para la evaluación del riesgo pasaron por alto darle prioridad a los activos como el SIVRI o el Satélite. Deben darle la mayor prioridad porque en ellos reposa toda la información sensible y no sensible de toda la Vicerrectoría de Investigaciones.
Criterios para la valoración de las salvaguardas	① ② ③ ④ ⑤ Respuesta: 5
	Observaciones:
Criterios para el tratamiento de riesgos	① ② ③ ④ ⑤ Respuesta: 5
	Observaciones:
Aceptación de riesgos	① ② ③ ④ ⑤ Respuesta: 5

Tabla D.2. Evaluación por parte de un experto

D.2. Encuesta de satisfacción al usuario

Según los autores de [64], la mayoría de los artículos publicados en relación con las ciencias de la computación, proveen poca o ninguna validación empírica. En razón de lo expuesto, se consideró que, además de ejercitar la adaptación para evaluar su desempeño como mecanismo para la gestión de riesgos de la SI, se debería realizar una encuesta de satisfacción del usuario que permitiera reforzar la validación de la adaptación. La decisión de usar encuestas se fundamenta en [64, 93, 94, 95, 96], donde sus autores destacan dicha herramienta como un instrumento eficaz que permite incrementar la calidad de los estudios empíricos mediante la adecuada validación de las soluciones.

En virtud de lo señalado, se desarrolló una encuesta de satisfacción del usuario que permitió validar los aspectos fundamentales de la adaptación de la metodología MAGERIT V3. La encuesta fue entregada, de manera impresa, al actual Jefe de la División de Gestión de Investigación, el señor Helder Chacón Villota quien, en su calidad de responsable del caso de estudio, termina siendo el usuario final de la adaptación. A continuación, las Figuras 6.12, 6.13 y 6.14 exponen los resultados de esta encuesta conformada por 12 preguntas que fueron formuladas con base en la escala de Likert [97]

ENCUESTA DE SATISFACIÓN DEL USUARIO

Con la presente encuesta se pretende medir el nivel de satisfacción del usuario de la adaptación de la metodología MAGERIT V3 como mecanismo para la gestión de riesgos de la SI en procedimientos que, como el caso de estudio, sean los encargados de gestionar proyectos de investigación en la Universidad del Cauca.

A continuación, la Tabla 1 expone las preguntas de la encuesta y la respectiva respuesta por parte del usuario de la adaptación, el Jefe de la División de Gestión de Investigación, el C.P[1]: Helder Chacón Villota.

NO	ENUNCIADO	RESPUESTA
1	La adaptación de la metodología MAGERIT V3 permitió identificar y clasificar, adecuadamente, todos los activos vinculados al caso de estudio.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo
2	La adaptación de la metodología MAGERIT V3 permitió valorar los activos de manera objetiva y reproducible, mediante el uso de criterios adaptados al contexto del caso de estudio.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo
3	Los resultados de la valoración de activos reflejan la realidad del caso de estudio.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo

Figura 6.12. Encuesta para la validación de la adaptación propuesta.

4	La adaptación de la metodología MAGERIT V3 permitió identificar y valorar satisfactoriamente las amenazas que atentan contra los activos vinculados al caso de estudio.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo
5	Los resultados de la valoración de las amenazas reflejan la realidad del caso de estudio.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo
6	La adaptación de la metodología MAGERIT V3 permitió estimar satisfactoriamente el nivel de riesgo al que se encuentran expuestos los activos vinculados al caso de estudio.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo
7	La adaptación de la metodología MAGERIT V3 permitió definir, adecuadamente, las prioridades de tratamiento de riesgos.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo
8	Los resultados de la estimación del riesgo reflejan el estado actual de la SI en el caso de estudio.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo
9	La adaptación de la metodología MAGERIT V3 permitió caracterizar satisfactoriamente las salvaguardas necesarias para mitigar los riesgos que atentan contra los activos vinculados al caso de estudio.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo

Figura 6.13. Encuesta para la validación de la adaptación propuesta. Parte II

10	Las salvaguardas seleccionadas permitieron mitigar satisfactoriamente los riesgos que atentan contra los activos vinculados al caso de estudio.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo
11	La adaptación de la metodología MAGERIT V3 define los roles y responsabilidades de SI considerando la estructura organizacional de la Universidad del Cauca.	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo
12	Gracias a los resultados obtenidos por el presente proyecto, se considera recomendable el uso de la adaptación de la metodología MAGERIT V3 para gestionar los riesgos de la SI en otros procedimientos encargados de gestionar proyectos de investigación en la Universidad del Cauca	● Totalmente de acuerdo ○ De acuerdo ○ Parcial ○ En desacuerdo ○ Totalmente en desacuerdo

Tabla 1. Encuesta de satisfacción del usuario

Para dar constancia de los resultados de la presente encuesta, firma a los 25 días del mes de Mayo del año 2016:

HELDER MAURICIO CHACÓN VILLOTA
C.C: 10.538.987
Jefe de la División de Gestión de Investigación
Vicerrectoría de Investigaciones
Universidad del Cauca

Figura 6.14. Encuesta para la validación de la adaptación propuesta. Parte III